Appendix A

Sector Summary Reports

Executive Order 13010 designated as *critical* certain infrastructures whose incapacity or destruction would have a debilitating impact on our defense or economic security. Eight were named: telecommunications; electrical power; gas and oil storage and transportation; banking and finance; transportation; water supply; emergency services (including emergency medical services, police, fire and rescue); and government services. Because some of the eight listed infrastructures lent themselves to similar approaches, the Commission organized into five study teams to address the infrastructure sectors and industries listed below. This appendix provides summaries of the five sector studies, which will be published as separate appendices to the Commission's report.

Information and Communications

Introduction

The US information and communications infrastructure (I&C) sector generates more revenue than most nations produce. Far more than any other nation, the potential of the new technologies has enabled the US to reshape its governmental and commercial processes. We have led the world into the information age, and in so doing have become uniquely dependent on its technologies to keep our economy competitive, our government efficient, and our people safe.

Background

The I&C sector includes the Public Telecommunications Network (PTN), the Internet, and the many millions of computers for home, commercial, academic, and government use. The PTN includes the landline networks of the local and long distance carriers, the cellular networks, and satellite service. Switches automatically establish and disconnect circuits between communicating parties on demand. Prior to the introduction of cellular service in 1983, virtually all switched service was provided by the wireline telephone system. The system's two billion miles of fiber and copper cable remain the backbone of the I&C sector, with the newer cellular and satellite wireless technologies largely serving mobile users as extended gateways to the wireline network. The PTN provides both switched telephone and data services and long term leased point-to-point services.

The Internet is a global network of networks interconnected via routers which use a common set of protocols to provide communications among users. Internet communications are based on connectionless data transport. In other words, the Internet protocol does not establish a circuit between communicating parties during the lifetime of the communication. Instead, each message is divided into small packets of data. Routers forward the packets to other routers closer to their destinations based on address information in the packet headers. To maximize efficient use of the network, the routers may send each packet of a message over a different path to its destination, where the message is reassembled as the packets arrive.

The Internet and the PTN are not mutually exclusive, since significant portions of the Internet, especially its backbone and user access links, rely on PTN facilities. Current trends suggest that the PTN and the Internet will merge in the years ahead; by 2010 many of today's networks will likely be absorbed or replaced by a successor public telecommunications infrastructure capable of providing integrated voice, data, video, private line, and Internet-based services.

The installed base of computers in the US has risen from 5,000 in 1960 to an estimated 180 million today, with over 95 percent of these being personal computers. The remainder includes the majority of the world's supercomputers and roughly half of the world's minicomputers and workstations. Networking of these machines through the circuits of the PTN and the Internet has grown exponentially over the past 15 years, creating an extended information and communications infrastructure that has changed the way we work and live. This infrastructure has swiftly become essential to every aspect of the nation's business, including national and international commerce, civil government, and military operations.

Threats

The reliability and security of the I&C sector have become matters of critical importance. The primary threats to reliability are natural disasters and system failures. The primary threats to security are deliberate physical and computer, or "cyber," based attacks.

Because they are generally well understood, somewhat predictable, and geographically confined, natural disasters are the most manageable of the threats to I&C reliability. In recent large scale emergencies, telecommunications systems have proven highly resilient. The current policies and organizational arrangements for dealing with natural disasters are working and require no modification at this time.

A second threat to infrastructure reliability, less predictable and potentially farther reaching, is system failure arising from increases in the volume and complexity of interconnection and the introduction of new technologies. The unbundling of local networks mandated by the Telecommunications Act of 1996 has the potential to create millions of new interconnections without any significant increase in the size or redundancy of network plants. Unbundling will be implemented at a time of rapid and large scale change in network technologies. The interaction of complexity and new technologies will almost certainly expand the universe of ways in which system failure can occur, and, unlike natural disasters, there is no assurance that such failures will be localized. Nevertheless, demonstrated system performance, ongoing research, and the ability to modify legislative and technical timetables suggest that the challenge will be successfully managed.

While rapidly increasing complexity has characterized the I&C infrastructure since the breakup of the Bell System and the advent of the Internet, system reliability has remained extraordinarily high. Large scale system failures have occurred very infrequently and have been corrected within hours.

The Federal Communications Commission (FCC) and the telecommunications industry have actively researched reliability issues throughout the 1990s, laying the groundwork for the expected influx of new service providers and technology vendors. Major players in telecommunications have maintained a vested interest in network reliability and can be expected, as in the past, to collectively maintain and improve network performance. Finally, the legislative and technical imperatives underlying the restructuring and can be modified if serious difficulties

arise. The current framework of FCC regulation and industry standard setting are self-imposed and are expected to prove capable of accommodating the challenges to reliability posed by complexity and technological advance. This framework can be extended beyond its traditional switched network focus to cover cellular, satellite, cable, and the Internet.

The third and least predictable threat to the infrastructure comes from deliberate attack. Depending on their objectives, attackers may seek to steal, modify, or destroy data stored in information systems or moving over networks, or to degrade the operation of the systems and networks themselves, denying service to their users.

Attackers include national intelligence organizations, information warriors, terrorists, criminals, industrial competitors, hackers, and aggrieved or disloyal insiders. While insiders constitute the single largest known security threat to information and information systems, controlled testing indicates that large numbers of computer based attacks go undetected, and that the unknown component of the threat may exceed the known component by orders of magnitude.

Adversaries can employ a variety of methods against the infrastructure, including traffic analysis, cryptologic attacks, technical security attacks, physical attacks, and cyber attacks. Of these, physical and cyber attacks pose the greatest risk. They have increased rapidly in sophistication and disruptive potential during the 1990s, while the infrastructure's vulnerability has grown. The availability of truck bombs, chemical agents, and biological agents has markedly increased the disruptive potential of physical attacks. At the same time, the vulnerability of the I&C infrastructure to physical attack has increased as service providers have concentrated their operations in fewer facilities.

In the cyber dimension, tools to remotely access, change, or destroy information in vulnerable systems and to control, damage, or shut down the systems themselves have become more sophisticated, easier to use, and more widely available. Department of Defense tests and exercises, together with the rising incidence of documented intrusions and cyber-related losses over recent years, indicate that networked computers are highly vulnerable to these techniques. A broad array of adversaries, including a sizable number of foreign governments, are currently capable of conducting cyber attacks. The Defense Science Board expressed a mainstream view in its November 1996 estimate that limited strategic information warfare capabilities against the US infrastructure will to emerge over the next seven to ten years.

Vulnerabilities

The critical functionality of the PTN—increasingly software driven and remotely managed and maintained—is vulnerable to cyber attack. Deregulation will markedly expand the access points from which to launch an attacks. New entrants will be permitted to interface with the local exchange carrier networks at many different points, including local loops, switches, trunk lines, common channel signaling systems, advanced intelligent network systems, and operating systems. Technical details of the systems are widely available. Open interfaces and common

communications protocols will make intrusion easier by standardizing targets and simplify the propagation of attacks from one location in the network to other parts of the architecture.

The introduction of numerous third parties, including foreign companies operating in partnership with US companies or on their own, into every aspect of network operations will alter the trust relationship on which current network architecture is based. The security measures needed to compensate for the loss of trust will take years to develop. During this time, attacks to gain unauthorized access to sensitive data and functions will be easier to accomplish on a widespread basis than at any previous time in the history of telecommunications.

Switching

The susceptibility of the current generation of switching equipment to software based disruption was demonstrated in the collapse of AT&T's long distance service in January 1990. A line of incorrect code caused a cascading failure of 114 electronic switching systems. We believe AT&T's accidental failure could alternatively have been triggered maliciously by relatively small individual actions. Successor generation switching equipment now entering service is likewise potentially vulnerable to remote access, alteration, or control by skilled attackers.

Transport

Another major vulnerability in switched networks is the transport architecture. Transport refers to the transmission facilities used to move traffic between switching and hub offices within a network. Virtually all new fiber optic installations by commercial carriers are currently being configured as Synchronous Optical Networks (SONETs). Most of the elements in SONETs are managed remotely through packet data network connections vulnerable to electronic intrusion. In addition, SONET elements can be remotely attacked through maintenance and testing ports. The first large scale network outage known to be caused by cyber attack was the disruption of a "bulletproof" SONET ring.

Signaling

Common channel signaling (CCS) networks are connectionless data packet networks that carry instructions for call setup, special services, billing, and all other functions involving more than one element across the network. The potential for software-based disruption of common channel signaling was demonstrated in June 1991 when phone service in several cities, including 6.7 million lines in Washington, DC, was disrupted for several hours due to a problem with the network's Signaling System 7 protocol. The problem was ultimately traced to a single mistyped character in the protocol code. Current methods of protecting CCS networks from spurious messages are adequate to detect minor intrusions but are insufficient to protect the network from serious attacks. CCS network elements are also potentially vulnerable to tampering through remote access.

Control

Network operations are controlled by network elements that carry out tasks based on information received via signaling messages or retrieved from network databases. Traditionally, service control for voice telephone service resided in the switches. Implementing new services required

physical rewiring of the switching fabric. In recent years, local exchange carriers have been moving service logic to special purpose processing and database systems outside the switches, where it can be upgraded quickly through software changes alone. This control architecture, which permits rapid creation of custom services, is called the advanced intelligent network.

The ability of service logic programs to change the way the network reacts to subscribers' calls makes them a potential source of disruption if they are misprogrammed, corrupted by accident, or accessed and altered by adversaries. Access to service logic of all kinds is set to expand markedly as a 1993 FCC notice providing for access to the advanced intelligent network by third party service providers goes into effect. The FCC ruling states that these service providers must have the ability to incorporate their own service logic and add their own hardware to the network. As the network becomes more open, interfaces to third party providers will provide many new points of entry into the network and its signaling systems, increasing the potential for accidental or deliberate misuse.

Management

Management refers to the tasks associated with running networks on a day-to-day basis, including configuration management and maintenance. These tasks are for the most part automated and carried out from central locations using computer-based operations support systems. Today's high levels of automation and interconnection of network elements make manual management of the network virtually impossible.

Operations support systems are susceptible to a variety of attacks. An attacker can delay, replay, or alter the order in which messages are received, triggering unauthorized management operations. An attacker can alter the contents of management messages, tricking a network node into accepting management parameters that may affect the operations or configuration of the node, interfere with accounting, or disrupt traffic. An attacker can simply prevent exchanges between a managing node and its managed nodes, disrupting network operations.

In the coming years, as subscribers demand greater control over their network services, providers are expected to offer configuration management capabilities unprecedented in today's networks. Misuse of these more powerful capabilities will have the potential to disrupt or halt communications over significant portions of the network.

Network maintenance is increasingly performed through remote access. Remote access allows maintenance personnel to electronically access distant network elements to perform maintenance or management functions. Eliminating the need to physically dispatch repair personnel allows faster response to problems and more efficient use of maintenance staff. The channels used for remote access by authorized maintenance personnel offer potential attack routes for adversaries. Once logged on, an attacker can remove nodes from service and disrupt the network.

Operations support system capabilities have continued to increase in sophistication and in the number of network elements they can control simultaneously. The trend is to reduce the number of operations support systems in the network while expanding their ability to provide a multilevel view of network operations. This has led to the creation of megacenters, which concentrate op-

erations for large segments of the PTN and data communications networks in one location. A megacenter may service central offices extending over a multistate region, giving its operators access to every switch, operations system, and maintenance channel in the central offices served. An adversary with electronic access to a megacenter could target individual circuits, bring down selected services, or disrupt normal operations over large areas.

Another growing vulnerability in network management is the trend by public switched network service providers to manage network elements via the Internet. The Internet was originally built as a vehicle for information sharing in an open and cooperative environment. Security was not a primary design consideration. With its relatively uniform structure and uncomplicated protocols, the Internet offers less resistance than the public switched network to systematic attack. Its growing use in network management offers adversaries the opportunity to attack the PTN by disrupting the Internet. Improved security should be a key priority for the Next Generation Internet.

Findings

Today's level of threat and degree of vulnerability present two risks for national policy to address. The first is the cumulative risk generated by myriad small scale attempts to steal information or money through cyber attack. The vulnerability of individuals and enterprises to cyber theft damages the nation's current and future competitiveness. Losses undermine both the bottom line and public confidence in emerging information technology. For the information and communications infrastructure to realize its full potential as a medium for commerce, government, and military operations, users must have confidence that transactions will be confidential and protected.

The numerous security vulnerabilities in today's I&C infrastructure afford little basis for such confidence today, and the trends are not encouraging. In the meantime, the payoff for successful exploitation is increasing rapidly. With commerce growing exponentially over a medium with minimal protection, criminals and hackers can be expected to develop original and profitable new methods of operation. With larger and larger quantities of imperfectly protected information residing on networked systems, intelligence services and industrial competitors can be expected to find increasingly sophisticated ways to break in. To the extent they succeed, we lose competitiveness. To the extent we are forced to retrench in reaction to losses, we sacrifice opportunity.

The second and more critical risk is that presented by cyber and physical attacks intended to disrupt the US I&C infrastructure and the critical societal functions that depend upon it. With network elements increasingly interconnected and reliant on each other, cyber attacks simultaneously targeting multiple network functions would be highly difficult to defend against, particularly if combined with selected physical destruction of key facilities.

The possibility that such disruption could cascade across a substantial part of the PTN cannot be ruled out. Our experience with very large scale outages is extremely limited, and has dealt with reliability problems rather than deliberate and repeated attack. Network resilience has been as-

serted, but large scale testing is not feasible. Computer models capable of systematically analyzing security risks associated with large telecommunications networks have not been developed. No one knows how the network would react under coordinated attack. We do know that relatively minor software problems have produced cascading failures in the past. We cannot confidently set an upper limit on the disruptive potential of a planned, large scale campaign.

As the scale and objectives of potential cyber campaigns become more focused, their feasibility and potential for success increases. Achieving selected outages of regional targets, such as financial districts or ports of embarkation for deploying forces, is feasible for a greater number of adversaries than a major disruption of the national infrastructure, particularly if they have access to physical as well as cyber weaponry. Achieving outages of selected equipment, such as high density network elements serving large customer populations, is even more feasible. Noting the large scale outage achieved in a recent cyber attack on a SONET ring, widespread denial of service through remote attack is now a demonstrated capability.

To address the risk posed by the mounting incidence of cyber theft and other small scale attacks, national policy must encourage a cooperative approach to strengthening the security of the infrastructure. To address the risk posed by the vulnerability of the infrastructure to widespread disruption, national policy must ensure that there is an effective national capability to detect and defend against large scale attacks on the I&C infrastructure.

Recommendations

The US has led the world into the information age, and in so doing has become critically dependent on its technologies to conduct national and international commerce, governmental functions, and military operations. The protection of the US information and communications (I&C) infrastructure is a vital national interest.

Six years ago, the National Research Council's report *Computers at Risk* described the growing vulnerability of networked computers and outlined a series of core principles to improve security. Progress in implementing these principles has lagged, while vulnerability and threat have grown significantly. The vast expansion of computer networking, the increasing dependence of the PTN and the Internet on computer-based, remotely-managed control elements, and the increasing levels of interconnectivity and complexity mandated by the Telecommunications Act of 1996 have created new vulnerabilities to I&C reliability and security. Natural disasters, accidents, and system failures pose growing threats to infrastructure reliability, while increasingly powerful methods of physical and cyber attack pose growing threats to infrastructure security. With the I&C infrastructure having become vital to every critical economic, social, and military activity in the nation, effective action to implement effective assurance practices is a matter of great urgency.

Our I&C infrastructure encompasses a wide range of activities extending over vast reaches of physical and virtual space. No entity in government or industry directly controls more than a

small fraction of it. The problem of infrastructure security will require shared effort across organizational boundaries. No organization can solve it alone.

Implementing infrastructure protection policies is neither an entirely public nor an entirely private responsibility. The risks are common to government, business, and citizen alike. Reducing those risks will require coordinated effort within and between the private and public sectors. The need for infrastructure protection creates a zone of shared responsibility and cooperation for industry and government. If we are to retain and build upon the competitive edge information technology has given us, we need to work together to substantially improve the trustworthiness of our information systems and networks.

Strengthening Security Through Cooperation Between Industry and Government

To strengthen the security of the information and communications infrastructure, the Commission recommends that the federal government work in cooperation with industry to:

- Strengthen overall public awareness to gain acceptance of and demand for security in information systems.
- Promote the establishment and rapid deployment of generally accepted system security principles, beginning with those concerning password management and imported code execution.
- Promote industry development and implementation of a common incident reporting process.
- Increase accessibility of government threat and vulnerability information, expertise in system security assessment and product evaluation, and operational exercises to assist government and industry risk management decision making.
- Define and maintain metrics for security, along with the current set of reliability metrics, for public telecommunications networks.
- Actively promote network assurance research and development.
- Establish an international framework to support the use of strong cryptography on a global basis.
- Promote the development of effective security enabled commercial information technology and services. Accelerate the development and implementation of usable, affordable tools, methodologies, and practices in information security.
- Support uniform “one call” legislation against the “backhoe threat.”

Defending Against Attack

An effective capability to defend the I&C infrastructure against attack in both the cyber and physical dimensions will require new sensing and warning capabilities, an organizational structure capable of dealing with the ambiguities of cyber attack, and new technologies for cyber defense. To ensure that there is an effective national capability to detect and defend against large scale attacks on the information and communications infrastructure, the Commission recommends that the federal government:

- Establish a focal point for national security policy on information infrastructure assurance and a focal point for national operational defense.
- Develop and sustain a robust intelligence collection, analysis, and reporting capability against cyber threats.
- Partner with private industry in developing and implementing indication and warning capabilities.
- Develop technologies needed for defending the nation's infrastructures against cyber attack, including after-action analysis and criminal investigations.

Leadership by Example

To serve as a national model for sound information assurance practices, the federal government should meet or exceed all applicable industry-based best security practices in building, operating, and using its portions of the information and communications infrastructure. Specifically, the Commission recommends that the federal government:

- Implement a common interdepartmental macro-level information systems security policy to standardize procedures and accountability.
- Require participation by all departments and agencies in annual information system vulnerability assessments, online security testing, and operational exercises.
- Establish clear visibility for information system security expenditures in the budgets of departments and agencies to facilitate management.
- Provide appropriate training and professional education in information assurance for all federal system managers, operators, and users, and assist state and local governments in establishing similar programs.

Physical Distribution

Introduction

The physical distribution infrastructure is critical to the national security, economic well being, global competitiveness, and quality of life in the US. The vast, interconnected network of highways, railroads, ports and inland waterways, pipelines, airports and airways facilitate the efficient movement of goods and people and provides this nation a distinct competitive advantage in the global economy.

Transportation is a major component of the US economy, representing in 1995 approximately $777 billion, or 11 percent of the Gross Domestic Product (GDP). US commerce depends heavily on the export, import, and domestic movement of raw materials, manufactured goods, foodstuffs, and consumable supplies.

The physical distribution infrastructure includes almost 4 million miles of public roads and highways and more than 360,000 interstate trucking companies, 20 million trucks used for business purposes, and 190 million personal vehicles. It includes more than a hundred thousand miles of track operated by the largest railroads, with 1.2 million operating freight cars and over 18,000 locomotives. It includes airlines that carry more than half a billion passengers a year through 400 airports. It includes almost 6,000 transit entities operating rapid transit rail and bus services. It includes 1,900 seaports and 1,700 inland river terminals on 11,000 miles of inland waterways carrying grain, chemicals, petroleum products, and import and export goods. The physical distribution infrastructure includes more than 1.4 million miles of oil and natural gas pipelines. And it includes delivery services, such as the US Postal Service and many other commercial providers that deliver goods and products on time not only to households, but to manufacturers whose very survival depends on just-in-time delivery of materials and supplies, and to business and even military activities who depend on the rapid delivery of repair parts to keep them in operation.

In this country, transportation is a matter of choice, and of intense competition. Commuters can choose between driving to work or taking mass transit. Travelers can choose to fly, catch a train or bus, or drive the highway. Shippers have their choice among highly competitive, customer focused delivery services and, in the deregulated world of transportation, among trucking firms, railroad companies, barge companies, and deep water shipping companies. Thousands of freight forwarders and consolidators, customs brokers and shipping agents move goods and cargo across the nation and through its ports quickly, cheaply, and effectively.

The US has the world's best transportation and distribution system, which both enables and reflects our having the number one economy in the world. Assuring that this system remains effective is critical to the well being of American citizens and the security of our nation.

Most of our nation's transportation infrastructure is owned by the private sector—railroads and pipelines; the vehicles and equipment operating on our roads, on the water, and in the air; and by state and local governments—our roads, airports, mass transit systems, and ports. The federal government owns the National Airspace System (NAS) operated by the Federal Aviation Administration (FAA), and the locks and dams operated by the US Army Corps of Engineers. The private sector is largely responsible for assuring its own infrastructure and business practices.

Trends

In the past, the business of transportation was conducted with paper—paper contracts and agreements, delivery orders, letters of credit, invoices, manifests, bills of lading, and shipping tags. Today, transportation, like other industries, is becoming increasingly enmeshed in our information-based society with its critical dependence on data and instantaneous communications.

While the transportation system has long been dependent on petroleum fuels, its dependency on other infrastructures continues to increase, for example, on electricity for a variety of essential operations and on telecommunications to facilitate operations, controls, and business transactions.

Demands on the physical distribution infrastructure continue to grow with the population and the economy. However, the ability to expand this infrastructure is limited. Rights of way for new roads, pipelines, railroads, and airports are difficult to obtain and justify. New means must be developed to make the existing system more efficient. Governments and industry have turned to information technology to increase that efficiency. Modernization of the NAS, extensive use and dependence on the Global Positioning System (GPS), and rapidly expanding use of Intelligent Transportation Systems (ITS) all will contribute to a more efficient transportation system.

Electronic commerce and data interchange, which make "just-in-time" delivery the norm rather than the exception, are increasing efficiency and giving companies a competitive edge in the global economy. However, requirements for open access to energy system data, increased dependency on data bases, and placing Supervisory Control And Data Acquisition (SCADA) systems on the public telecommunications network make these systems more vulnerable to unauthorized intrusion. The explosion of telecommunication requirements and intense competition in the communications infrastructure are leading to greater volumes of traffic on existing lines, thereby increasing the potential for "single point failures."

Railroad companies continue to merge, consolidating operations centers and lines, moving more and more traffic onto fewer corridors, and reducing the redundancy of the networks and increasing their vulnerability to physical attack.

Natural gas is being moved by existing pipelines without any agency or organization having a clear picture of the entire system or an understanding of its ability to handle surges in demand, or the tools necessary to evaluate the impact of a system-wide disruption.

The air traffic control system of the FAA is based on decades old technology. The replacement system, while doubtless more efficient, will be more vulnerable unless special security measures are incorporated.

Congestion is common in most metropolitan areas; ITS are being introduced to make more efficient use of existing road systems, but at the same time they will introduce new vulnerabilities. A discussion of the challenges specific to Emergency Services is provided later in this Appendix.

Public Expectations

The American public takes for granted freedom of choice among transportation modes and carriers, and generally wants government intervention limited to matters affecting safety and security. Transportation systems are expected to be reliable and predictable, designed and operated to allow unimpeded flow of goods through ports, across state and international boundaries, with rapid customs and immigration clearance processes and minimal regulatory and bureaucratic impediments.

Infrastructure maintenance and improvement must be adequate to ensure continued foreign investments in the nation's economy. A competitive level playing field within and between modes of transportation is crucial to freedom of choice and an efficient distribution system. Timely delivery of goods and products is essential, so we expect delivery services to be predictable and dependable. Government policies and regulations are expected to foster stability and consistency.

The public reluctantly accepts accidents involving planes, trains, and automobiles. But when the cause is found to be a failure of government oversight, such as substandard aircraft maintenance or a faulty traffic device, the public demands accountability. When a natural disaster affects the physical distribution infrastructure, the public expects rapid restoration. While the public anticipates and tolerates congestion on the nation's roads and highways, government is expected to use effective traffic management systems and techniques to minimize congestion. Gasoline, natural gas, and other energy supplies are expected to be available on demand.

Finally, the public expects a transportation infrastructure ready to respond to national crises, including adequate sea and airlift to move military forces quickly to any trouble spot on the globe.

Federal Role

The US Department of Transportation (DOT) provides national policy, funding, and safety requirements through its operating agencies:

- Office of the Secretary of Transportation (OST)

- Federal Aviation Administration (FAA)
- Federal Highway Administration (FHWA)
- Federal Transit Administration (FTA)
- Federal Railroad Administration (FRA)
- US Coast Guard (USCG)
- Maritime Administration (MARAD)
- Research and Special Programs Administration (RSPA)

DOT works to maintain the integrity of the US transportation infrastructure against terrorist and other criminal acts through a combination of regulations, guidelines, inspections, cooperative agreements, and government investments. Intermodal and interagency intelligence matters and security related actions are coordinated by and with the Office of Intelligence and Security within OST. Security actions are carried out by the DOT operating agencies, commensurate with their respective authorities.

The FAA, Coast Guard, and, to a limited extent, RSPA's Office of Pipeline Safety, are the only DOT agencies with clear statutory authority related to security.

Civil aviation security remains DOT's first priority and primary focus. The FAA has the responsibility and the authority to require contingency measures for air carriers and airports to deal quickly and effectively with immediate threats against civil aviation.

The Coast Guard has authority to respond to threats against cruise vessels and ports in the US and against vessels anywhere in the world carrying US citizens. The Coast Guard can institute regulations to establish and manage security zones around important facilities or operations, and to require certain port facilities and cruise lines to implement security measures.

RSPA regulates the design, construction, testing, operation, and maintenance of natural gas and hazardous liquid pipelines and liquefied natural gas (LNG) facilities; specific security authority exists only for LNG facilities.

Security authority and contingency plans for land transportation, including mass transit, railroads and highways, tunnels and bridges, and for a major portion of the nation's pipeline system, do not exist within DOT. Millions of people use passenger rail daily, and as shown by the 1995 Aum Shinrikyo gas attack in Tokyo and bombings of the subway system in Paris, mass transit remains open and vulnerable to terrorist acts. Millions of miles of pipelines carry natural gas and other hazardous materials throughout the country, and are largely unprotected and vulnerable to sabotage. Railroads carry tons of hazardous materials through heavily populated areas with little consideration given to the possible impact of intentional attack. Despite the possible national level political implications of a terrorist attack, protection of railroad, highway, and mass transit facilities remains the responsibility of industry or state and local governments.

Threats and Vulnerabilities

Transportation is inherently vulnerable to a wide range of physical threats. Natural disasters such as floods, earthquakes, landslides, and hurricanes are ever present; when these disasters strike, services are restored through the combined efforts of federal, state and local governments and the affected industry. As for man-made threats, with the exception of civil aviation, few countermeasures are available or appear to protect our transportation systems from physical attack by terrorists or other criminals. In the event of disruption from man-made causes, reconstitution and recovery are the responsibility of the owners and operators of the systems.

While the prospect of physical disruptions has been with the physical distribution infrastructure since its infancy, transportation industries are only beginning to focus on information-based threats or attacks. Many business systems are demonstrably vulnerable; this problem must be addressed by industry. To make intelligent decisions, however, industry leaders need current information on new and emerging threats. This information may be held within other companies in the same industry, in other industries, and within various agencies of the federal government.

Governments and industry have turned to information based systems to increase the efficiency of the public/private transportation system. While these increased efficiencies help keep our industries and companies competitive in the global economy, businesses are now much more vulnerable to electronic penetrations and attack and to disruptions of their supporting infrastructures, particularly telecommunications and electric power.

Conclusions and Findings

Today, information-based attacks cannot cause trains and planes to crash, nor are they likely to cause pipelines to rupture. Tomorrow—perhaps next year, perhaps in ten years—critical transportation systems could be vulnerable to such attacks and crippled unless action is taken now.

Roles, Missions, and Responsibilities

The Department of Transportation has been extremely proactive in counterterrorism efforts, both within the federal government and with the transportation industry. However, based on the Commission's outreach to industry and the federal government, several shortfalls in transportation infrastructure assurance, other than counterterrorism, have been identified:

- No defined roles, mission, and responsibilities for DOT in infrastructure assurance related areas other than counterterrorism.
- Lack of awareness and extremely limited availability of education programs.
- Incomplete or absence of vulnerability assessments of both physical and information-based portions of the transportation infrastructure.
- Limited and untested dissemination of threat information and warnings, and absence of an effective program to share critical information within the industry, and between the industry and the federal government.

- Absence of joint federal government/industry contingency or response plans to respond to an infrastructure threat or attack.
- Absence of security or assurance standards, guidelines, or best practices.

DOT is not well positioned to support the industry in infrastructure assurance efforts. The federal government must be involved with prevention, recovery, and reconstitution efforts within the transportation sector. DOT is neither funded nor staffed to address, with the industry, current or emerging threats to transportation.

Data Collection

Accounting for about 20 percent of all terrorist attacks around the world, transportation systems are a favorite target of terrorism. Better information and data on attacks would assist in development of countermeasures and provide better information for risk management decisions. Some modes of transportation are required to report all safety related incidents and accidents above a certain threshold, while others report through insurance agreements. These data are used to establish programs that can prevent and mitigate incidents and lead to cost effective improvements in safety. The private sector, however, is reluctant to report information-based attacks, fearing public disclosure of vulnerabilities that could be exploited by others and have a negative impact on public confidence in the industry. The physical distribution community is not an active partner in the improvements of data processing and communication systems, and as a result, has become more vulnerable with the extensive adoption of these systems.

Information Sharing and Threat Dissemination

Transportation is essential to the national economy and national security. Transportation is a high visibility terrorist target. Yet no agency or private sector organization is required to have, nor actually has, a program to advise the industry of information-based threats and attacks, nor are intrusions or attacks on the transportation infrastructure generally reported to the federal government.

No tested and effective means exists that facilitates reporting and transfer of information between the government and transportation infrastructure stakeholders on threats and attacks. Information-based threats to the physical distribution system are not addressed by DOT; private sector concern is on a sector-by-sector and company-by-company basis. Established reporting systems, where they do exist within the government and the transportation industry, are "stovepiped," and are not sufficiently shared or coordinated with DOT or with established national indications and warnings processes. Neither the federal government nor the private sector is tasked with identifying, quantifying and tracking information-based threats and attacks, nor is any organization responsible for analyzing and disseminating that data.

The apparent lack of information and sharing about information-based attacks on physical distribution systems limits industry understanding of the extent of the problem and makes it difficult to justify investment in measures to prevent or mitigate the impact of information-based attacks.

Industry representatives who receive information from DOT say they need more on the threat. The DOT is required by statute to notify the civil aviation industry of terrorist threats, but the statute does not require the DOT to notify the remainder of the transportation industry of threats.

Identification of Critical Assets

While industries are aware of critical assets within their companies, the federal government (e.g., DOT) has not identified and does not track those assets critical to the national security. Government/private sector contingency plans generally do not exist for responding to a terrorist threat or attack on the transportation infrastructure. While the transportation industry in general is capable of responding to natural disasters and other similar disruptions to their systems, coordinated plans to evaluate and/or respond to threats of a coordinated series of attacks on the transportation infrastructure have not been developed.

The transportation sector must be aware of and develop a process to protect key assets during heightened threat conditions.

- While the federal government is familiar with some of these assets, industry is in the best position to identify those facilities that require protection during national security events.
- Railroad, airline, highway, port and pipeline operation centers, among other facilities, are critical.
- A coordination process is essential to develop protection and recovery contingency plans.

The National Airspace System (NAS)

The present NAS is relatively immune from intrusions. It is composed of difficult-to-penetrate, dedicated subsystems, with the subsystems having different designs and older, specialized versions of software. However, the modernized NAS will undergo major new developments, including open systems architecture, and will depend on communications technology that permits wide interchanges of information among many of its subsystems.

The NAS would likely become a prime target for terrorism and “rogue” nation states during a national defense emergency.

Because the modernized NAS appears to be particularly at risk from information-based attacks; the FAA and Congress must take firm action to ensure adequate security measures are implemented with the new system.

1) The threat of attacks on the NAS subsystems has been low to date. There have been isolated incidents, including phantom controllers, during and immediately after the 1981 controller strike, and more recently at Roanoke, VA. While the FAA subsystems have not been subject to information warfare in the past, portions of the system still are vulnerable. For example, there have been recent instances of contractor use of FAA communications systems to access and modify software code under development and test.

2) Today's older NAS subsystems have some protective mechanisms built in to trap and remove damaged messages, unauthorized message types, and excessive flight plan filing activity. The subsystems also have many dedicated networks and different versions of proprietary software and communications protocols that make it difficult for intruders. But, their susceptibility will become more severe as the new NAS subsystems are installed.

3) During transition to the future NAS architecture, the level of vulnerability may increase as new systems elements are added to the NAS.

4) The nature of air traffic control operations provides a strong countermeasure that exists in real time within the NAS. Air traffic controllers are constantly observing the traffic under their jurisdiction and pilots are aware of unusual flight circumstances. This controller and pilot detection of system abnormalities will still be important in reducing the impact of any future attacks on the NAS subsystems.

5) The major vulnerabilities inherent in the new architecture are the planned use of new open systems and, using shared communications networks. Use of these new architectures, in conjunction with commercial off-the-shelf (COTS) hardware and software products, will increase the risk of insider and outsider (hacker) access, and the probability of malicious actions that interfere with the operation of NAS subsystems. These actions include data and software corruption, virus and Trojan horse damage. Use of shared networks will significantly increase the FAA system vulnerability to outside attack.

6) Systems with air-ground communications and data links such as the Automatic Dependent Surveillance-Broadcast mode (ADS-B), the Air-ground Data Link (ADL), and the Wide Area Augmentation System/Local Area Augmentation System (WAAS/LAAS) are susceptible to interference and signal jamming.

7) In the past there was a lack of priority and funding for establishing and conducting a security management program in the FAA, and for implementing information security protection for new automated and open system architectures. The situation is improving in that the top FAA managers forming the Joint Review Council (JRC) have recently identified a need for funding security provisions in the NAS, and have made a preliminary estimate of the funding levels to be included in future FAA budget submissions.

While the FAA has initiated the above effort to address security requirements for the NAS during its upgrade, the security improvements are currently unfunded and need Administration and Congressional support.

Pipelines

Two federal agencies perceive an assurance responsibility for the nation's pipeline system, presenting a unique situation as follows:

- DOT is statutorily responsible for regulating pipeline safety, and in some cases, for security.

- The Department of Energy (DOE) is statutorily responsible for oversight of the nation's energy supply; and as such has in place an effective intelligence and threat dissemination system.

These sometimes overlapping responsibilities must be clarified.

Regarding pipelines, current Environmental Protection Agency (EPA) efforts to publish "worst case scenario" data on the Internet raise serious concerns about the availability of targeting information for both terrorist and nation states. Access to this data should be controlled and made available to the public only on a limited basis. All federal agencies, not just DOT, and the industry, must consider the impact of making potential target information easily and readily available on the Internet and through other anonymous means; at a minimum, access must be controlled on a need-to-know basis.

Global Positioning System (GPS)

The Federal Radionavigation Plan calls for GPS and its augmentations to be this nation's sole radionavigation system by 2010. Current plans, if not modified, could lead to an over reliance on GPS based systems for critical transportation functions. The modernized NAS will depend on GPS and GPS augmentations as its sole navigation and landing systems. Exclusive reliance on any single system creates inherent vulnerabilities; no single system can be guaranteed for 100 percent availability for 100 percent of the time. Possible exclusive reliance on GPS and its augmentations, combined with other complex interdependencies, raises the potential for "single point failure" and "cascading effects."

Recommendations

Agency Roles, Missions and Responsibilities

The Commission is recommending that lead agencies be designated to promote the development of information sharing in respective sectors. Each designated lead agency would take a leadership and coordinating role with the private sector, and also seek appropriate legislation that allows for infrastructure assurance. The DOT, in assuming its responsibilities as sector lead for the Physical Distribution Infrastructure, should consider:

1) Establishing a central office responsible for coordinating intermodal infrastructure assurance as well as terrorism issues, including prevention, mitigation, contingency response, and recovery, and for coordinating with modal and other federal agencies, acting as primary contact points with industry on assurance issues.
2) Developing joint government/industry response and recovery plans with the private sector.
3) Establishing an improved information dissemination and sharing process.
4) Testing the effectiveness of the dissemination process and of established security procedures.

5) Working closer with industry on R&D and education.

6) Requesting for funding and positions to manage these emerging issues and responsibilities.

7) Reviewing of all proposed legislation for adherence with infrastructure assurance policies.

8) Obtaining appropriate executive and legislative authorities necessary to accomplish Lead Agency responsibilities.

Specific funding is necessary within OST and within individual DOT agencies for the following:

1) Providing government security clearances to industry, particularly for CEOs and CIOs.

2) Developing security and infrastructure assurance education programs.

3) Performing cross-cutting research on assurance issues, including GPS, the NAS, and train control systems, and for interagency research with agencies such as NASA and the Department of Defense (DoD).

4) Developing security standards or guidelines, and reporting systems.

5) Using secure telephones (STU III's), and encryption, strengthened firewalls, and other security measures.

6) "Red Teaming" and testing of critical DOT systems and industry systems on a co-operative, selective basis.

7) Conducting DOT sponsored industry symposia and workshops.

Education

Information security programs in the nation's business schools are very limited. Federal sector leads should promote and support development of undergraduate and graduate level programs and courses of instruction, including information security, with concentration in their specific sectors.

Pipelines

The Commission recommends the DOT and the DOE establish a formal process for addressing pipeline assurance issues in partnership with industry, clearly defining the responsibilities of each Department for security related processes, including threat dissemination, coordination, appropriate federal response to threats, possible establishment of threat levels, and developing plans for addressing potential and actual long-term, serious disruptions in the nation's energy supply.

Global Positioning System

The Commission recommends the Secretary of Transportation:

1) Fully evaluate actual and potential sources of interference to, and vulnerabilities of, GPS before a final decision is reached to eliminate all other radionavigation and aircraft landing guidance systems.

2) Sponsor a risk assessment for GPS-based systems used by the civilian sector, projected from now through the year 2010.

3) Base decisions regarding the proper federal navigation systems mix and the final architecture of the NAS on the results of that assessment.

The DOT and FAA must develop a better understanding of interference and other vulnerabilities of GPS before a final decision is reached concerning the status of all other radionavigation and landing guidance systems. A federally sponsored thorough, integrated risk assessment would lay a sound foundation for decisions on future courses of action.

The National Airspace System

The Commission recommends the FAA act immediately to develop, establish, fund, and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions, intrusions and attack. Program implementation should be guided by the recommendations found in the *Vulnerability Assessment of the NAS Architecture*, prepared for the Commission. The Vulnerability Assessment included the following recommendations:

General:

1) The FAA must clearly define responsibility for information security and accountability within its organization. The leadership should be able to make risk decisions that have budget and operational impacts. The FAA has established a NAS Information Security Group (NISG) to coordinate the information security activities of their many organizations, but the group does not yet have decision making authority on the information security (INFOSEC) that will be implemented in the NAS.

2) The FAA should enhance its security protection program with such traditional practices as: implementing and rigorously enforcing a highly visible security policy; planning countermeasures for known open system and COTS weakness; identifying and drawing from emerging infrastructure protection concepts; maintaining a Red Team for independent protection verification; providing an adequate level of electronic security staffing; and establishing a program for security education, training and awareness.

3) The FAA should consider the implementation of full "trusted" hardware and software security capabilities for only the FAA's most vulnerable future subsystems, since the software cost for embedded applications, together with full audit, tracking, and monitoring, may be too great if applied to all subsystems. Relaxation of the full capabilities, such as less rapid revalidation (e.g., a slower fifteen minutes down time) and less constant vigilance of data integrity, should be considered on a case-by-case basis for less critical subsystems, particularly in situations where existing air traffic control recovery procedures exist.

4) The FAA should conduct a comprehensive investment analysis of NAS INFOSEC in order to determine the degree of security protection that is needed.

5) The FAA should program funds for security provisions for the most critical subsystems in the range of two to four percent of subsystem cost, with additional funds as these subsystems become operational. The FAA should refine these percentage estimates and the identification of the subsystems they apply to, through a study of risk mitigation consequences, the degree of penetration testing needed, and INFOSEC life-cycle costs.

Automation: The FAA should provide virus protection, software distribution protection, and access control protection during the design, development, testing, and life cycle support of the future subsystems. Banner or warning screens should be used on all areas accessed by outsiders on computer and communications networks.

Communication:

1) Design the communications networks of the NAS in such a way that interconnections between the FAA administrative network and the NAS operational networks are kept to an absolute minimum and use well managed state-of-the-art protection methods including firewalls.
2) Monitor the use of Internet for backup communications, now in its preliminary planning stage, to avoid intrusions during systems outages.
3) Continue to use dedicated circuits for the most critical NAS assets.
4) Provide comprehensive security protection and maintain a physical separation between the Administrative Data Transmission Network (ADTN) and the Internet, and maintain a physical separation of this network from all critical operational subsystems. The current architectural plans call for multiple ties to the Internet. Computers used for administrative purposes at operational facilities should have no connection to any operational system.
5) Provide backup communications links and standby service contracts to support satellite communications links that fail or are jammed or flooded. The backup links should be capable of the automatic assumption of communications.
6) Ensure that Internet uses from computers that are connected to operational systems are avoided or have strict high-level approval and accountability for access to these systems.
7) Use encryption (never a complete solution for security requirements) on all critical communications links that have National Security implications (future and actual flight plans for Presidential aircraft, and key governmental and military officials).

Navigation and Landing:

1) Establish and maintain a backup navigation and landing system capability, possibly retaining elements of the current navigation and landing systems.
2) Provide full or partial backup for satellite uplinks for the WAAS system.

Surveillance: Provide surveillance backup for the ADS-B system, particularly in high density terminal areas, and in the center of the continental US, where primary radars are scheduled for removal.

Intelligent Transportation System

The Commission recommends that the DOT develop security standards or guidelines for ITS to assist agencies and companies in designing security into ITS systems during development and installation phases.

Crime

The Commission recommends that an intermodal forum, sponsored individually or jointly by industry or the DOT, be established to address the issue of criminal intrusion into unsecured shipping company databases and electronic data interchange, and the potential impact on critical business practices. The forum should be used to bring this issue to the attention of senior government officials and corporate management, assess the scope of the problem, and share best practices.

Anti-terrorism Legislation

The DOT has submitted legislation (H.R. 1720, the "Surface Transportation Safety Act of 1997") designed to protect the passengers and employees of railroad carriers and mass transportation systems and the movement of freight by railroad from terrorist attacks. The Commission recommends this legislation be given strong support from the Administration and Congress.

Energy

Introduction

The security, economic prosperity, and social well being of the US depend on a complex system of interdependent infrastructures. The lifeblood of these interdependent infrastructures is energy, the infrastructure composed of three distinct industries that produce and distribute electric power, oil, and natural gas. Profiles of these three industries are shown in Figures A-1, A-2, and A-3.

In addition to being a key component of the other infrastructures, the energy infrastructure is critical to our economy, with estimated revenues from retail sales of electricity in the US exceeding $200 billion annually, and revenues from oil and gas almost $400 billion. US energy consumption by fuel type is depicted in Figure A-4.

Today our energy infrastructure is the most reliable and robust in the world. While energy shortages and outages have made national and international news, they are rare. The handful of major incidents in modern times, dating back to the 1965 Northeast Blackout, includes the gasoline shortages of 1973 and 1979 and the electric power outages in the western US in 1996. Despite the proven reliability of the US energy infrastructure, however, there are significant challenges to sustaining this robustness and resilience in the near future.

Disparities in prices across the country are partially responsible for the recent restructuring of the electric power industry and natural gas industry (Figure A-5). New information systems for electronic commerce, for data interchange and for improving operational efficiencies are now essential business elements of the energy infrastructure. Electric utility and natural gas companies are merging and consolidating resources, while at the same time new transmission line rights-of-way are almost impossible to obtain because of the “not in my back yard” syndrome or environmental concern. With the advent of natural gas and electricity commodity markets, the number of marketing companies has grown exponentially, from eight in 1992 to more than 250 in 1996, while electric power capacity reserves continue to shrink. As in the telecommunications industry, the customer of the electric power industry faces a complex service industry in which no one company will provide end-to-end service.

The reliability of electricity has become more critical to our nation’s competitiveness and standard of living in the Information Age. The use of natural gas to generate electricity is growing rapidly, as it is the current clean fuel of choice. And we are becoming ever more dependent on the supply of foreign oil, recently surpassing the 50 percent level for oil imports.

While the nation’s dependence on less expensive foreign oil continues to grow, refineries in this country are being closed and, in light of thin profit margins and environmental constraints, no

new refineries are planned in the US. Over the last decade the oil industry has lost 450,000 US jobs to overseas operations, and one major company alone has reported a workforce reduction from 30,000 to 20,000 employees during the early 1990s. Some of these job losses are blamed on federal and state environmental regulations. To minimize costs and increase efficiency, many companies are dramatically expanding their automation and networking systems and are linking their control, administrative, and business information systems. Many companies are also consolidating their computer centers, with one major worldwide company consolidating its operations into a single megacenter.

Most physical threats to the energy infrastructure are well known and documented. As a result of concern about terrorists attacks, the National Security Council, Congress, the Department of Energy (DOE), and the energy industry focused on the physical security of the infrastructure during the 1980s. This activity led to public hearings by Senator John Glenn of Ohio in February, 1989, and was documented in the Office of Technology Assessment report "*Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage.*" In response to the government's concerns, the energy industries compiled internal lists of their critical assets and spare components. Processes were established to disseminate threat information, selected security personnel were cleared to receive classified information and forums were established to share information. As a step toward ensuring viability of energy infrastructures, DoD and the Federal Bureau of Investigation (FBI) initiated their Key Asset Protection Programs. Joint private sector and government exercises were conducted for mutual education and to test the emergency response capabilities.

As farsighted and laudable as these efforts were, however, interdependencies within the energy infrastructure and with the other infrastructures were not studied, nor was the energy sector's growing dependence on information systems. Without electric power other critical infrastructures, such as telecommunications and banking and finance cannot function. The transportation infrastructure would cease to operate as it relies almost exclusively on oil products. These linkages reflect the growing interdependencies between the infrastructures.

Some analysts postulate that the 1996 western power outage and the New England and MidWest summer power shortages were not isolated instances, but are indicators of an industry experiencing a weakening in its historically strong assurance program.

Threats

Threats to the US energy system arise from a number of sources including hostile governments, terrorist groups, other organized groups or individuals, disgruntled employees, malicious intruders, complexities, natural disasters, and accidents. More than a thousand reported incidents directed against the US energy system have been documented by the DOE over the last 15 years; some involved outages and significant damage. In recent years, cyber incidents, including deliberate as well as accidental malfunctions, have begun to appear.

Organized attacks on the energy infrastructures in other countries include an Irish Republican Army (IRA) plot to blow up energy and water installations and cause massive disruption across

London in the summer of 1996. A police raid in south London found 36 devices; the planned targets included six electrical substations, gas valves and pipelines, and water pumping stations. Six participants were found guilty of conspiracy and were sentenced to 35 years in prison. A more recent event occurred in Texas this April, when a group planted explosive devices on three natural gas holding tanks at a processing plant to divert police attention during a robbery attempt. It was believed the explosions would have released toxic fumes which could have wiped out half of the county.

The most common disrupter of energy supplies is inadvertent damage to buried cables or pipelines, such as is frequently caused by a "back hoe." However, these disruptions are usually localized and have no national level impacts.

Downsizing of the industries, partially in response to restructuring and consolidating pressures, leads to a significant loss of expertise that is difficult to replace. Downsizing also disrupts the traditional compact between employer and employee and creates a potential cadre of disgruntled "insiders." An estimate provided to the Commission by industry security directors was that 75 to 80 percent of the security incidents they experience are caused by persons from within the organization.

Managing consequences of natural disasters and accidents is an inherent part of the energy industries' operational processes. Their mitigation and response efforts and activities have high public visibility, and have resulted in an outstanding response by the industry.

Vulnerabilities

Specific areas of vulnerability addressed by the Commission's Energy team are categorized as:

- Electric Power: power generation (including fuel supply) systems, transmission systems, distribution systems, electric network control and protection systems.
- Oil and Natural Gas: supply, transportation, storage and distribution (pipelines are a joint effort with the Commission's Physical Distribution team).

The Commission's review focused on those elements of the infrastructure in which exploitation of a vulnerability could cause extended regional or national impacts. Nominal impact figures used were 500,000 people/customers affected for at least 12 hours.

Vulnerabilities facing the energy industries include:

- Those created in the operating environment by the rapid proliferation of industry-wide information systems based on open-system architectures, centralized operations, increased communications over public telecommunications networks and remote maintenance;
- Supervisory Control and Data Acquisition (SCADA) systems that are vulnerable because of use of commercial off-the-shelf (COTS) hardware and software, connections

to other company networks, and the reliance on dial-back modems that can be bypassed;

- Increased availability of vulnerability information, much of which is mandated by regulatory bodies to facilitate competition, and the tools for exploiting those vulnerabilities;
- Rapid assimilation of advanced technologies with their inherent complexities;
- Consolidation of infrastructure corridors (e.g., communication, electric transmission lines, pipelines, etc.); and
- Previously identified physical vulnerabilities of critical assets that have not been adequately addressed throughout the industry.

Electric Power Vulnerabilities

Of particular concern are the bulk power grid (consisting of generating stations, transmission lines with voltages of 100 kV or higher, plus 150 control centers and associated substations) and the distribution portion of those electric power systems whose interruption could lead to major metropolitan outages. (Note: this report covers the "grid," a North American system comprising the US, Canada, and a small part of Mexico.) On the cyber side, the focus was on the larger networks, including those that interconnect a company's information and operation systems and those that interconnect company systems to each other (Figures A-6 and A-7).

The most significant physical vulnerabilities appear to be related to substations, although certain generation facilities and transmission lines are also inviting targets. There is general agreement that since the industry designs for stability during single and certain double failures, a coordinated attack on multiple targets would be required to cause a significant disruption of service. Furthermore, such an attack would need to hit multiple targets simultaneously or in rapid sequence.

Because of the complexity of the grid, attackers would have difficulty replicating cascading outages such as the two western power outages of July and August 1996. More research is needed to better understand the dynamics of the grid, particularly the phenomenon of voltage collapse, which can lead to a cascading outage.

From the cyber perspective, SCADA systems offer some of the most attractive targets to disgruntled insiders and saboteurs intent on triggering a catastrophic event. With the exponential growth of information system networks that interconnect the business, administrative, and operational systems, significant disruption would result if an intruder were able to access a SCADA system and modify the data used for operational decisions, or modify programs that control critical industry equipment or the data reported to control centers.

Oil and Gas Vulnerabilities

Large refineries (greater than 250,000 barrel capacity) in California, Texas and Louisiana would be attractive targets for physical or cyber attack. The significant increase in the proportion of oil transported via pipelines over the last decade provides a huge, attractive, and largely unprotected target array for saboteurs. Elements of the pipeline system that could be targeted include lines at

river crossings, interconnects, valves, pumps, and compressors. Three major pipelines in the country offer the greatest potential for significant impact if attacked successfully. However, on the positive side, over the last five years, many interconnections have been added to natural gas pipelines, making rerouting around a break easier, but this may not always be possible if the line is at capacity.

As in the electric power industry, SCADA systems used in the oil and gas industries are subject to electronic intrusion. If accessed, information could be manipulated or control programs modified. Under certain circumstances, a hammering effect could then be induced in pipelines, possibly leading to breaks. More research is needed to determine the feasibility of such attacks.

Status and Assessment of Current Energy Infrastructure Assurance Programs

The DOE is the lead federal government organization for response to energy emergencies but has limited authority in the infrastructure assurance area. The Federal Energy Regulatory Commission (FERC) oversees wholesale electric and gas rates and service standards, as well as the transmission of electricity and gas in interstate commerce. The North American Electric Reliability Council (NERC) has assumed primary private sector responsibility for the reliability of the bulk power system (that is, the portion of the electric utility system that encompasses the electrical generation resources and transmission system shown in Figure A-1). The Security Committee of the Edison Electric Institute (EEI) provides a forum with a focus toward physical security and law enforcement activities for the security directors of investor owned utilities. The National Petroleum Council (NPC) is an advisory committee of 175 CEOs from the oil and gas industries, and the American Petroleum Institute's (API) and American Gas Association's (AGA) Telecommunications Committees provide forums for telecommunications specialists. The Electric Power Research Institute (EPRI), the Gas Research Institute (GRI), and the Institute of Gas Technology (IGT) are the leading energy technology organizations. The DOE National Laboratories are another source of significant expertise for solutions to the complex technical problems associated with infrastructure assurance.

As a result of the restructuring of the electric power industry, NERC has made significant changes to its organization, including the new requirement of mandatory compliance to its policies and procedures, compliance monitoring, enforcement measures, and increased and broadened membership. However, since NERC is a voluntary organization, enforcement is questionable. Also, a tension exists between different industry groups.

Another notable effort is the Secretary of Energy's Task Force on Electric System Reliability, which was recently established to provide advice on ways to address key institutional, technical, and policy issues associated with maintaining bulk electric system reliability in the new era of a competitive electric industry. An interim report, published in July, focuses on institutional recommendations to enhance overall reliability of the electric power system.

The critical components of the energy infrastructure remain vulnerable to physical attack, and replacement of many of these components involves lead times measured in months. However, most major companies have improved the physical security of their critical sites. From a cost benefit perspective, the companies believe they have taken prudent measures. Many companies' restoration programs are tested all too frequently by nature (hurricanes, earthquakes, tornadoes, fires, and floods) and existing mutual aid agreements have enabled restoration of service in reasonable time, even after the worst disasters.

From the cyber perspective, much needs to be done, and many issues have arisen, of which there is only limited awareness. Even the leading companies have only recently focused on information assurance issues. Despite increasing concern about vulnerabilities, many companies are understaffed in the cyber security area. Where cyber security experts are employed, their main focus appears to be on the business data processing side of the company, with a large share of their effort being expended on virus contamination problems. In most companies, information systems (business, administrative, and operations) are being networked, both internally and externally. Although many industry officials are aware of the significant vulnerabilities introduced by connecting to the Internet, most companies are making such connections. However, in attempts to provide security for information systems, many companies are placing confidence in individual measures, such as firewalls and dial-back modems, to secure their networks. The Commission's studies show that a more systematic approach is needed.

Several proactive information assurance efforts should be noted. The NERC has recently undertaken an initiative to collect information on cyber intrusions. EEI has volunteered to work with other interested groups to further scope the issues and activities in the cyber security area of the electric power infrastructure. EPRI has taken the lead in cyber security for the electric power industry, while DOE has assumed the lead for the federal government. For example, EPRI and DOE have joined forces to assess the security design and development of the information system of the Independent System Operator recently established in California. Also, DOE's Office of Nonproliferation and National Security has outreach programs on cyber security, energy emergencies, and threat assessments. Another notable effort was the three day seminar conducted by IGT (Emergency Response and Critical Infrastructure Protection in the Gas and Electric Industries) in June 1997.

Findings

1) The authorities and responsibilities for energy infrastructure assurance in the federal government need to be clarified.
2) The respective responsibilities of government and private sector for infrastructure assurance are not clearly understood.
3) Improved sharing of threat information and "indications and warning" (I&W) information is needed. Improved sharing of industry experience is needed (e.g., a fully populated cyber intrusion database).

4) More training and awareness in infrastructure assurance is needed, focusing on risk management, vulnerabilities, performance testing, and cyber security.

5) Infrastructure assurance technology advancements could add significantly to the overall protection of industry assets.

6) Adopting uniform physical and cyber security guidelines, standards or best practices would enhance protection.

Recommendations

Energy Infrastructure Assurance Strategy

Historically, the energy infrastructure's strategy has focused on robustness and resilience. The physical vulnerabilities of the pipelines and transmission grid are widely acknowledged and understood, and the philosophy has been to mitigate the natural and man made events that can exploit those vulnerabilities so that service to the customer is not interrupted or, if interrupted, only for the shortest possible time. To assure the energy infrastructure in the future, owners, operators, and the government must work together to develop a strategy focused on the primary objectives of prevention, mitigation and recovery.

Owners and operators can further expand communication channels with the government for sharing information on threats and vulnerabilities to ensure that they are making informed risk management decisions; enhance their research and development, focusing on cyber security and reliability projects; and as major customers of the telecommunications and software industries, make demands for more secure products and services.

Government agencies can contribute to the prevention, mitigation, and recovery of infrastructure losses by assuring that appropriate information sharing paths are established between owners/operators and the government; that existing or new regulations do not adversely impact the protection of the infrastructure; that a level playing field exists for the industry to invest in long term preventive measures; that threat and vulnerability information is provided to assist industry in making informed risk management decisions; and that long-term research and development activities are conducted to enhance assurance.

Implementation of Assurance Strategies

The Commission recommends:

1) Expanded roles and responsibilities for owners and operators, and the government to provide balance for the recommended strategy.

Owners and Operators

- Provide CEO level advisory counsel on infrastructure assurance issues, much as NSTAC provides advice for telecommunications. Representation could come from EEI and NPC.

- Provide threat dissemination and information sharing through associations such as NERC, API, INGAA and AGA.
- Formalize cyber security activities through such organizations as EEI, NERC, EPRI, API, and AGA.
- Fund enhanced infrastructure assurance near-term R&D through such institutions as EPRI and GRI.
- Emphasize education, training, and awareness using such resources as NERC and IGT.
- Provide a forum for development of enhanced physical and cyber security standards/guidelines through such organizations as the Institute of Electrical and Electronics Engineers (IEEE).

Federal Government

- Provide national direction through planning, policy, and legislation to maintain a level playing field for owners and operators investing in infrastructure assurance. Emphasize technology research, training and awareness, emergency response, and information sharing efforts.
- Develop and promulgate a mandated energy infrastructure assurance mission for the Department of Energy to address the responsibilities of the leadership and coordinating role as a federal government lead agency.
- Clarify the respective roles and responsibilities for pipeline security between the Departments of Energy and Transportation (DOT) through a joint effort.
- Provide enforcement/oversight for industry (electric power) reliability standards through FERC.
- Direct and fund the DOE National Laboratories to focus their expertise on infrastructure assurance assessments, response, and energy infrastructure assurance research and development (R&D).
- Expand the existing process for reporting power outages and physical attacks to include cyber attacks, and develop a legislative process to protect sensitive industry data.
- Develop and coordinate an enhanced process for timely, detailed threat information dissemination through the law enforcement and intelligence communities.

State Governments

- Provide assistance in the areas of training and awareness, and assurance exercises.
- Encourage the National Association of Regulatory Utility Commissioners (NARUC) to work through its member state commissions to enhance the protection of public utility infrastructures.

2) Owners, operators, and the government increase funding for R&D in the following technology related areas with security dimensions.
   - Cascading effects leading to voltage collapse.
   - Online security assessment, including online power flow and transient analysis.
   - Transmission and distribution technology, and real time control mechanisms.

- Large scale modeling and evaluation of the power grid and pipeline systems (regional and nationwide).
- Examine solutions to foreign energy supply vulnerability as a cost-benefit approach.

3) Secretary of Energy provide planning, policy, coordination, technical expertise and training/awareness for infrastructure assurance by:
   - Developing an energy infrastructure assurance plan in a coordinated government/private sector forum.
   - Encouraging development of physical and cyber security standards/best practices within the industries through the various associations (NERC, EEI, EPRI, IEEE, GRI, AGA, and API).
   - Developing and enhancing training, education and awareness programs for energy infrastructure assurance practitioners.
   - Providing the technical capability for vulnerability assessments available from National Laboratories to conduct reviews of critical infrastructure assets.
   - Funding a test bed/pilot program for energy infrastructure assurance that includes the private sector and government.
   - Coordinating with the private sector and DoD on research and development of risk management software and techniques, information assurance software and hardware for real time intrusion detection, enhanced authentication and authorization, and vulnerability assessment tools with a focus on SCADA systems.
   - Lead an industry/government effort to define the level of threat (e.g., criminal, insider, experienced hacker with intrusion software development capability) to be established as a goal for industry to defend against.

4) The Commission recognizes the importance of the following industry recommendations and recommends the Secretary of Energy work with the industry to:
   - Establish standards for a national “one call” program to address third party interruptions (dig-ins).
   - Continue joint effort between federal government, EEI, EPRI, NERC, and the oil and gas industries to further develop issues and activities pertinent to cyber security.
   - Review government regulations that require excessive reporting and release of what industry considers sensitive information (e.g., FERC Form 715 — Annual Transmission Planning and Evaluation Report).
   - Review regulations that may inhibit efforts by utilities to aid one another in emergency response efforts.
   - Form a permanently staffed center, jointly supported by government and industry, for sharing threat and vulnerability information from both public and private sector sources.

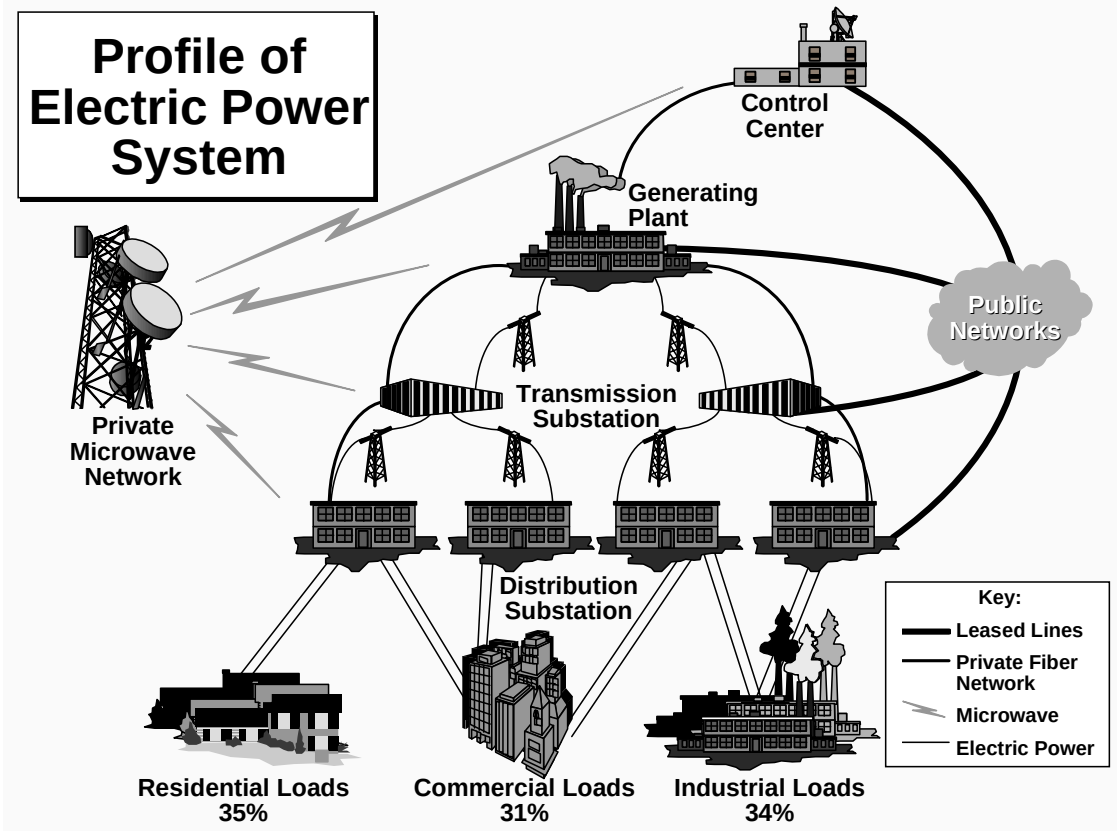


Figure A-1. Profile of Electric Power System

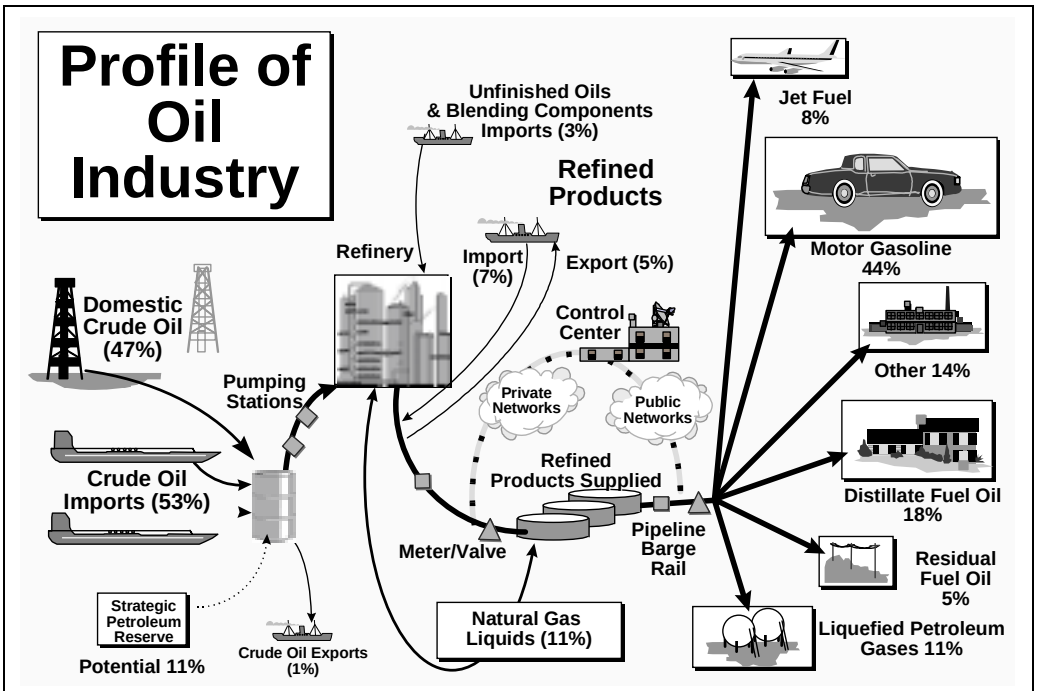


Figure A-2. Profile of Oil Industry

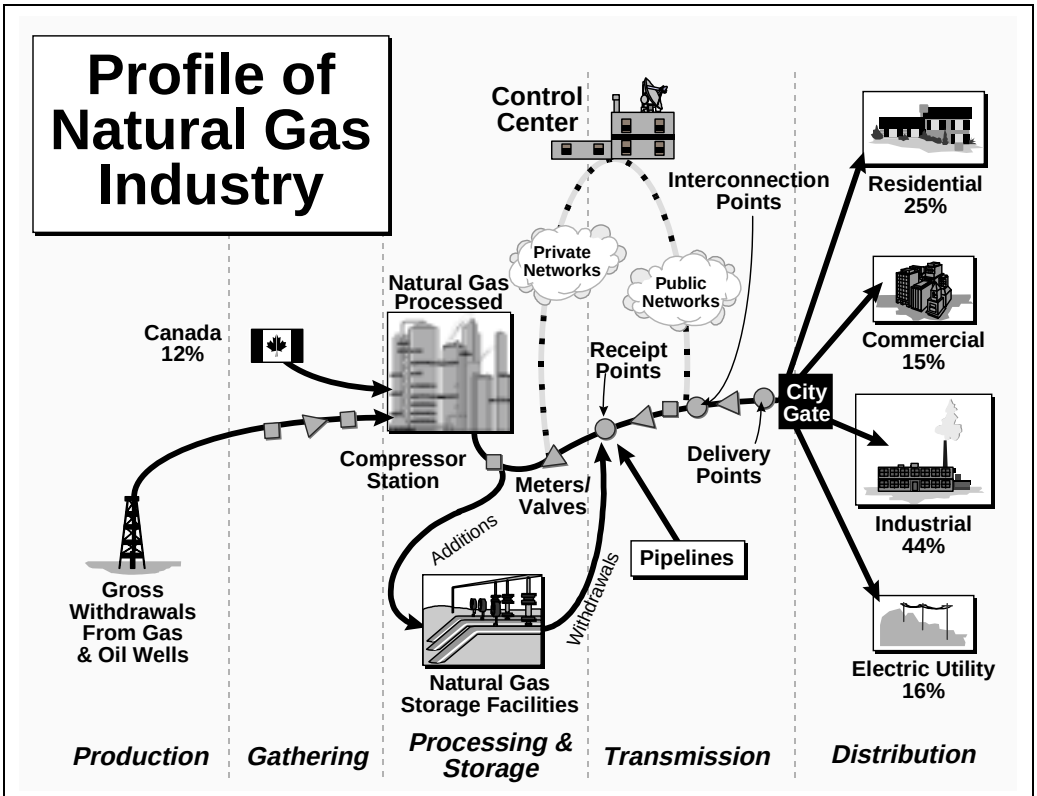


Figure A-3. Profile of Natural Gas Industry

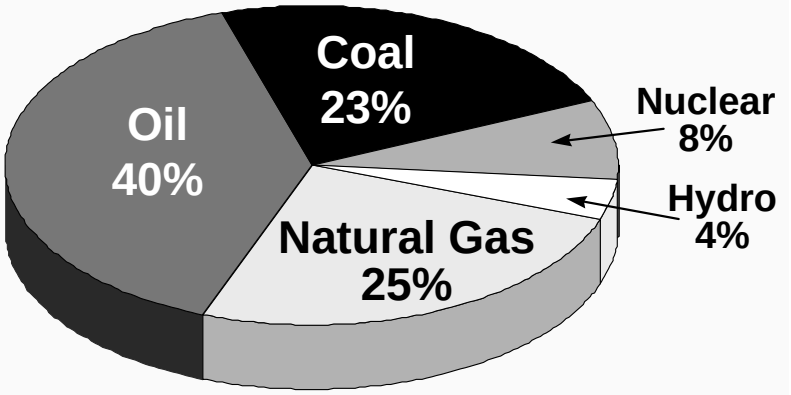
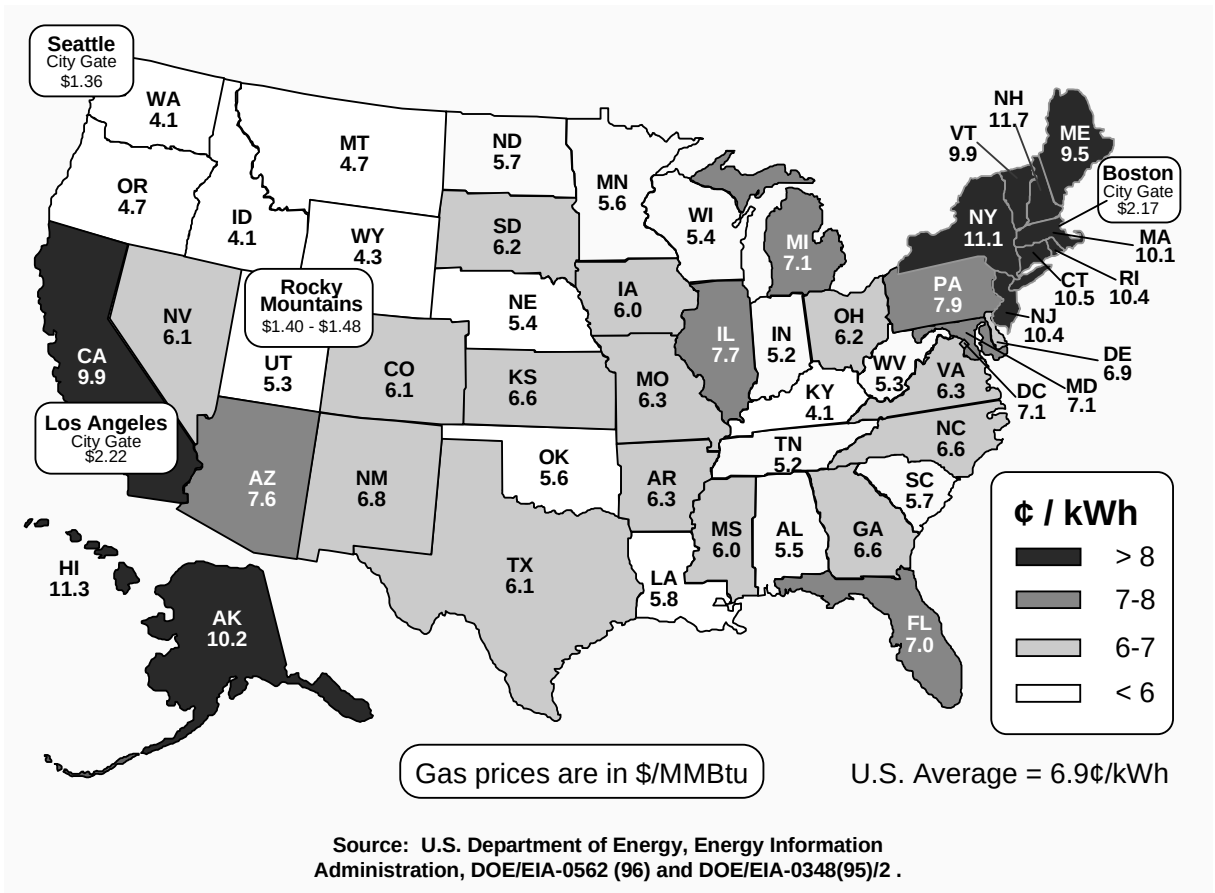


Figure A-4. US Energy Consumption



Source: U.S. Department of Energy, Energy Information Administration, DOE/EIA-0562 (96) and DOE/EIA-0348(95)/2 .

Figure A-5. US Electric and Natural Gas Prices

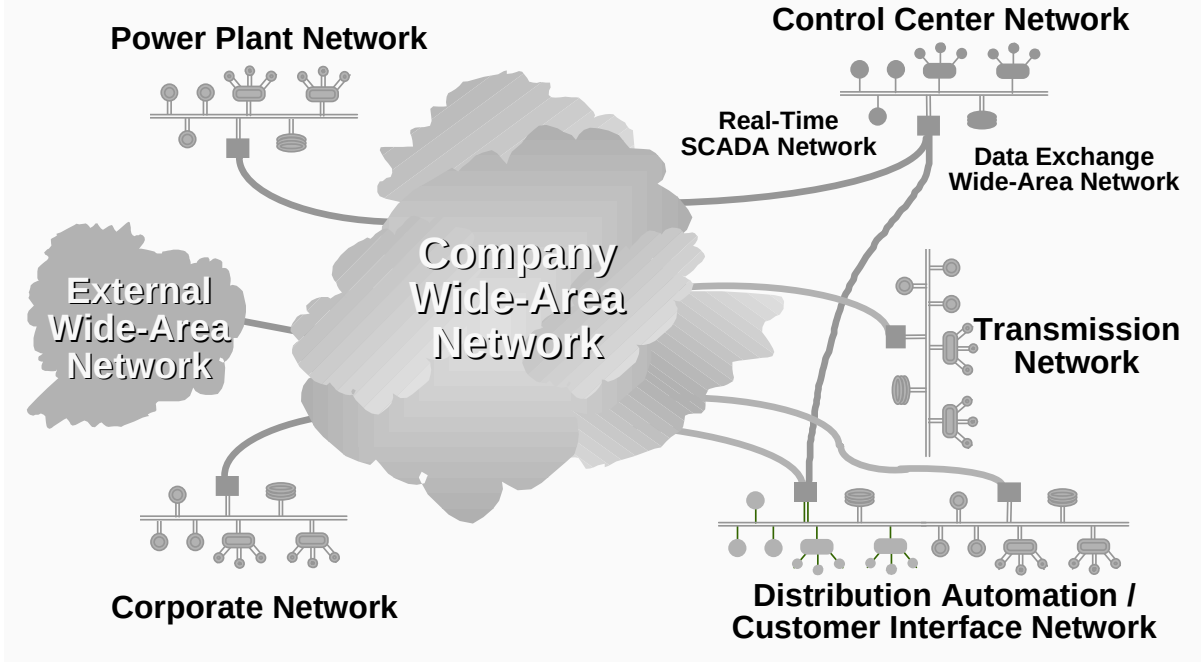


Figure A-6. Integrated Utility Network

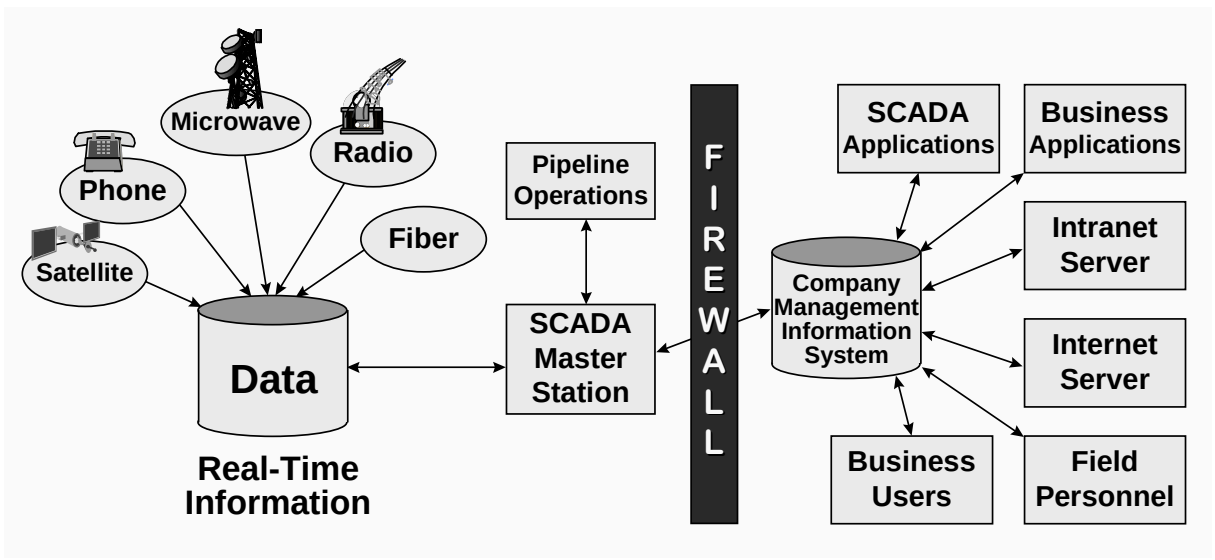


Figure A-7. Oil/Gas Current Internal System Configuration

Banking and Finance

Introduction

The US financial system is central not only to the functioning of domestic and global commerce, but to the daily lives of virtually all Americans. It represents bank holdings of about $4.5 trillion, a capital market of $7 trillion, investment bank underwriting of $1 trillion, almost $3 trillion in daily payment transactions, and about 10 million jobs.

More than a billion credit cards in circulation in the United Stated account for $500 billion in annual expenditure, or roughly half of all consumer debt. Also, due to the rapid increase in individual retirement accounts of various kinds and the popularity of mutual funds, about half of all households in the United States are investors in the stock market.

The banking and finance infrastructure was defined by the Commission as composed of five principal sectors: banks, financial service companies, payment systems, investment companies, and securities and commodities exchanges. The Commission's banking and finance team conducted a broad-based industry outreach, developed a profile of major participants, geographically mapped industry operations, assessed the level of vulnerability and defense extant within the financial system, and reviewed the analytic structures in prevalent use for such key industry processes as risk analysis and countermeasure investment decision-making.

Our principal finding is that, due to its carefully structured mixture of public oversight and private initiative, the US financial system is among the world's finest. The modern US financial system never has suffered a debilitating catastrophe, and for that reason among others carries an extraordinarily high level of global confidence. Some observers go so far as to characterize it as shock proof.

The Current Situation

The institutions comprising the financial services industry are further ahead than most in employing sophisticated and, in some cases, unique defenses against loss of assets and corruption of core data systems. Consequently, the US financial system is unusually well protected at the national level, and is well prepared to confront a broad range of threats to its operations and integrity.

However, along with other infrastructures studied by the Commission, the banking and financial service industry is undergoing significant structural change. Expansion by banks into previously prohibited business areas such as securities trading; mergers and acquisition activity; heavy and

growing engagement in dynamic global financial markets; and the steady move toward electronic commerce combine to present new challenges to the ways vulnerabilities are defined and risks and managed. And, at the operating level, heightened reliance on global information infrastructures and the advanced computing technologies which power them makes the management of those risks more complex.

Deregulation within the telecommunications and electric power industries upon which financial services so heavily rely introduces new factors to the industry's traditional risk management models. Multiple intermediaries have been inserted into what once were end-to-end service systems that—when combined with decreases in reserve capacity margins in these industries resulting from competitive cost pressures—make the operational interdependency among these three gigantic infrastructures even more opaque and complicated.

Risk Management

Managing risk is the principal business of financial institutions. They view protection against physical and cyber threats as a necessary cost of doing business, and they often position security as a competitive advantage and highlight it in advertising designed to attract new customers for such services as remote banking. Security is an integral component of institutional performance and accountability.

Security investments by financial institutions are driven by two primary forces.

- Law and Regulation: Mandatory investments made by the institution for legal or regulatory compliance. Because financial institutions are so heavily regulated, examination processes drive most security investments.
- Risk Management Analyses: Based on internal and external audit findings, industry and technology norms, history and current events, and estimates of future technology or threats, institutions evaluate risk according to probability of occurrence and the likely consequences for the institution. Security investments are made accordingly.

To assist in broadening the industry's recognition of new threats and vulnerabilities that could affect their risk assessments, financial institutions would benefit from better access to reliable current information from government and from across the industry. Reporting is generally compartmentalized by sector; only a few trusted mechanisms now exist for sharing the kinds of information needed to facilitate system-wide risk assessments.

Threats

The major current threats to the overall operation of the financial system are largely physical in nature, consisting either of natural disasters or a direct coordinated attack on the system's more vulnerable points. These are aggravated by the more open availability on the Internet of the kind

of information needed to plan such attacks, increasing reliance on global outsourcing of core operations, and the consolidation of bank and other operations centers as a result of merger and acquisition activity.

At the institutional level, however, the most persistent security threat is the insider who might use authorized access to confidential information or operating systems for profit. Financial institutions employ comprehensive and intricate systems of internal controls to counter this threat, but the knowledgeable insider dedicated to corruption is difficult to stop.

There is also the evolving threat of a larger scale cyber attack by a sovereign adversary or organized terrorists with the aim of inflicting serious damage on key elements of the US financial system. The current probability of this threat is estimated to be low but growing, and one of its more troubling features is that its source may be undetectable and the attack itself might be masked as a series of lesser intrusions.

Vulnerabilities

It is important to note some key distinctions in describing financial system vulnerabilities.

First, there is the distinction between vulnerability of the US financial system and opportunities for theft and fraud in individual institutions. Almost all media reporting on vulnerability up to now has risen from single cases of theft. Emblematic of this is the much reported access of Citicorp's electronic money transfer operation by a transnational criminal group in 1994. While this case made dramatic news accounts and was embarrassing to Citicorp, whose ultimate loss amounted to $400,000, it in no way reached the level of a threat to the bank, much less the financial system.

Second, there is the distinction between the financial condition of a single participant in the financial system and the strength of the system as a whole. Recent years have seen some spectacular financial events, such as the Mexican Peso crisis, the failure of Barings Bank due to fraud, and major scandals involving Japanese banks. These shocks were absorbed and managed by appropriate market, regulatory, and central bank actions without lasting harm to the full system.

Based on the sector profiles developed by the Commission, the nation's core payment systems (FedWire, CHIPS, SWIFT) and the organized securities and commodities exchanges seem to present a serious physical vulnerability within the financial system. This is so not because they have failed to take extensive precautionary measures, but rather because there is substantial cross sector dependence on the services they provide, and few if any alternatives available to provide those services in the event of a disabling catastrophe. In contrast, our analysis shows that the other sectors of the financial infrastructure have sufficient diversity to provide for the dispersion of risk among a wide range of alternatives.

As a countermeasure, the FedWire, for example, maintains three hardened operating centers capable of carrying the full volume of its wire transactions. Similarly, the New York Stock

Exchange (NYSE), as the nation's most influential exchange, has established extensive system redundancy, alternate power sources, and diverse communication links. Still, the physical concentration of its data processing and operations centers makes more plausible the possibility of an event or series of events that could disable both sites. Even in that event, however, contingency trading arrangements required by the Securities and Exchange Commission (SEC), although never tested, have been described by the SEC as able to restore NYSE operations within several days. Other major exchanges, such as the Chicago Board of Trade and the Chicago Mercantile Exchange, have similar recovery plans, as do lesser securities exchanges.

Public Confidence

Financial institutions are acutely aware that public confidence is their most critical asset. In that respect, the financial service industry shares with government a fundamental dependence on public support for its viability. This linkage is the basis for the important role government has in assuring the safety and soundness of US financial system.

Because of its sensitivity, however, financial institutions generally oppose reporting which goes beyond the existing mandatory regulatory and law enforcement channels. While it is understandable that these institutions wish to avoid costly reporting requirements and potentially damaging disclosures, taking such a position fuels critics who claim that there are large unreported losses -- especially related to computer intrusions of various kinds. Any new mechanism for the exchange of information must establish an acceptable climate of trust and control which will encourage participation by financial institutions yet meet emerging governmental national security requirements for more coherent, systemic risk assessments.

Market Forces and Government Action

There is little doubt that ultimately market forces will generate the appropriate level of investment in risk management tools necessary to secure the financial infrastructure into the future. Nevertheless, the financial system regulatory changes under consideration by the Administration and Congress all have in common an important government role in setting ground rules for new forms of competition; providing a level of fundamental indemnity for customers of the system, thereby relieving companies of some risk; and protecting the public interest in the safety, soundness, and fairness of the system as a whole.

Market forces work best when businesses see the investment as a necessary cost of operation, as consistent with their concepts of risk, as providing a competitive advantage, and protecting their brand (Figure A-8 illustrates this process). In this context, one of the problems with sole reliance on market forces for long-term investments in research and development of security tools, for example, is the lack of actuarial data upon which the risks associated with new threats and vulnerabilities might be calculated. Neither can the benefits of the investment be specified. Consequently, the economics of long term prevention measures often works against their development.

For example, for such major preventive measures as the establishment of redundant communications systems for the industry to rely on in the event of a catastrophic telecommunications or electric power failure, or the construction of an alternate trading site for the securities exchanges, payoffs are not easily envisioned. In the absence of measurable risk, the net present value of such investments is minimal if not zero, and justifying present costs to shareholders, investors, and securities analysts by citing general benefits in the absence of clear risk or competitive advantage is not likely to succeed. Therefore, business on its own will not invest in the kind of ultra secure contingency measures usually found in the military or national security arena without either more information about the risk, or some other incentive.

Summary

The current security of the US banking and finance infrastructure is strong. The government, through regulation, plays a central role in assuring the financial system's safety, soundness, and fairness, but the industry itself has over many years developed a diligent culture of security. Both the role of government and industry diligence will continue even as governing statutes and regulations are changed, technology advances, and the industry restructures and competes in the global market.

However, it is important to note that scrutiny of the financial services industry goes beyond government regulation and law enforcement. Because of its centrality to the nation's economy and the daily lives of most Americans, the extraordinarily high value of its assets, and its high global visibility, the industry's operations and behavior are closely observed by securities analysts, investors, major customers, journalists, and the public in general. This provides powerful additional incentive for financial institutions to assure their integrity and take the actions necessary to continue to earn and retain broad public confidence, retain customers, and achieve growth.

Overall, industry risk management efforts concentrate on prevention of loss, with mitigation of loss following in importance. However, contingency planning also is a high priority, as disablement resulting from an attack or natural disaster remains the industry's largest current risk.

Cyber risks on a system-wide scale may emerge from the possibility of unforeseen instability in the telecommunications and electric power industries as they deregulate and disaggregate. On an institutional level, increasing use of electronic banking mechanisms, requiring multiple ports of entry and perhaps an entirely new infrastructure to accommodate the demand for rapid data recall and payment processing, will create new forms of risk to information systems. For example, connections to the Internet for this purpose present a risk of unauthorized access to operating systems if the Internet connection is not effectively partitioned by firewalls and other such tools. Banks and others are approaching this with caution, although the attraction is strong in terms of operational efficiency and expanded market reach.

In the longer term, risk emerges from the maturing of Information Warfare capability among organized adversaries who may wish to attack the US by destabilizing large portions of the finan-

cial system, and erode public confidence in it as well as in the capability of the US to defend against such attacks. Both the government and industry would significantly benefit from improved flows of threat and vulnerability information so that precautionary measures can be developed and deployed system-wide at a pace sufficient to provide an effective defense.

Recommendations

Information Sharing

Regulators, law enforcement officials, and industry associations should coalesce to establish a trusted forum for the exchange of relevant threat and vulnerability information so as to facilitate the assessment of risk on a system-wide basis.

Contingency Planning

Regulators and industry associations should sponsor strategic simulations designed to test the adequacy of existing industry recovery plans under a variety of conditions. These should feature the emerging risk factors of growing interdependence complicated by deregulation and global expansion of operations.

Insider Threat

Regulators, private auditors, and the industry should continue to work together to improve examination processes, audit practices, internal controls, and physical security measures to accommodate new kinds of risks and to help deter the insider threat.

Back-up Facilities

National security, law enforcement, and regulators should decide whether the establishment of such security measures as a contingency trading site for major exchanges, contingency data storage centers, and dedicated communications systems, the cost of which probably exceeds the reasonable business risk involved, are appropriate as government-funded national security measures.

Education

Industry associations may wish to take the lead in establishing information security education and awareness programs within academia and in the general public.

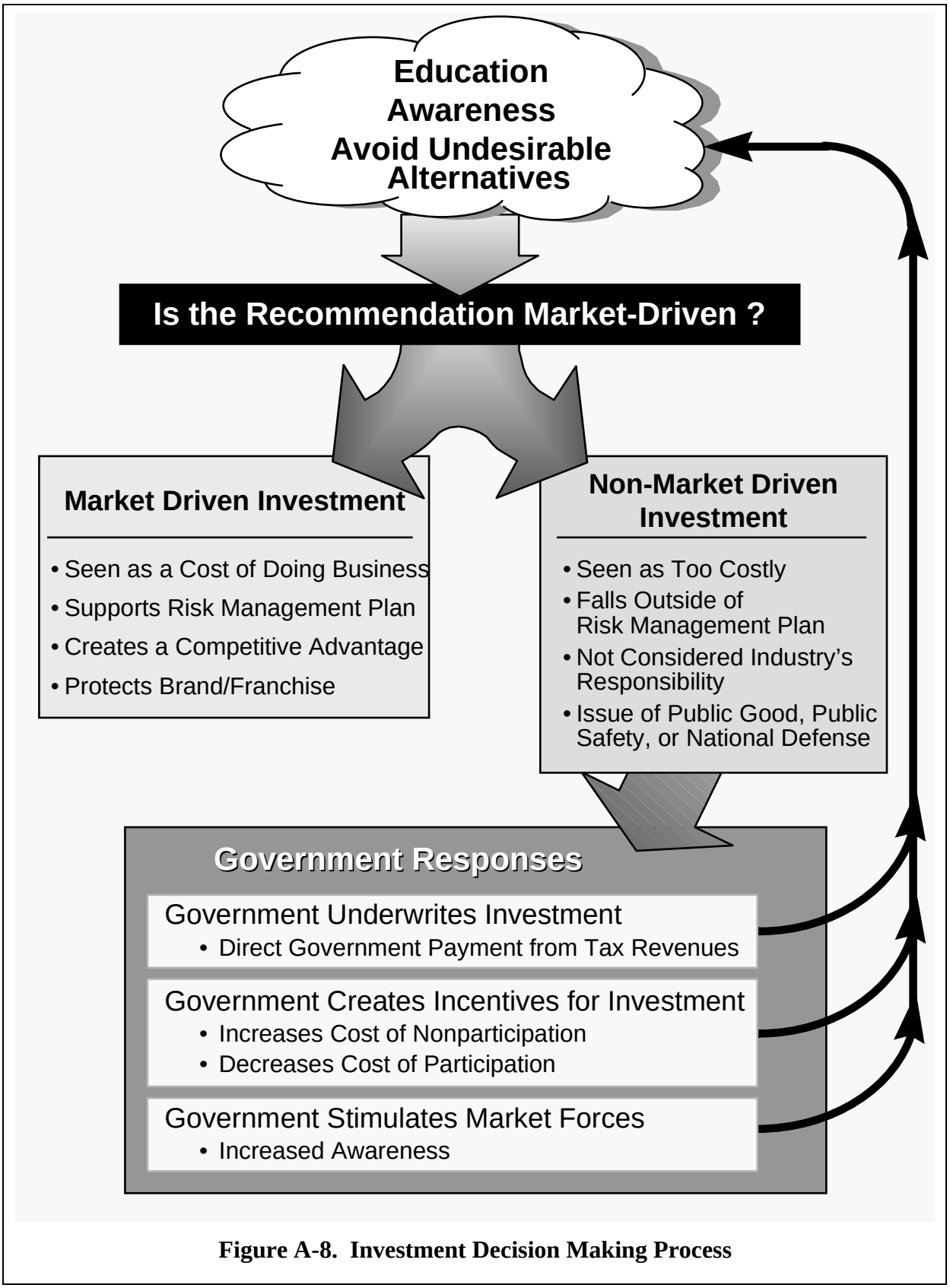


Figure A-8. Investment Decision Making Process

Vital Human Services

Introduction

The Vital Human Services (VHS) sector includes three of the critical infrastructures named in Executive Order 13010: water supply, emergency services, and government services. At the outset, the Commission considered expanding the scope of this sector to include food, health care and the nation's work force as additional critical infrastructures. However, because of time and resource constraints, the Commission decided to bound the scope of its effort to the eight infrastructures named in the Executive Order, leaving additional infrastructures to be considered in any follow-on activity.

The three VHS infrastructures differ from other named critical infrastructures in that they are focused largely at the local and state levels, are largely governmental responsibilities, and deal chiefly with human needs and safety. Because they are highly localized in character, they do not form a strongly interconnected national infrastructure. Failures in one community generally will be localized to that community. Nevertheless, they are critical national infrastructures and the problems and vulnerabilities faced in one community are similar to those faced in every community across the US.

Because these infrastructures relate directly to the populace, their disruption—or even threatened disruption—would have significant psycho-social effects. Loss of confidence in these infrastructures can greatly magnify the more objective costs to the economy and national security.

Water Supply

There is no "typical" water supply system for the US, at least not to any significant degree of detail. But, at a general level, all systems share five common elements.

1) A water source, either surface waters in impoundments such as lakes and reservoirs or flowing waters in rivers or ground water in aquifers.
2) Treatment facilities in which particulates are filtered out and disinfectants are added.
3) A system of aqueducts, tunnels, reservoirs, and/or pumping facilities to convey water from the source through the rest of the system and to provide storage and the means to balance flows.
4) A distribution system carrying finished water to users through a system of water mains and subsidiary pipes.
5) A waste water collection and treatment system.

The major uses of the water supply infrastructure are for agriculture, industry (including various manufacturing processes, power generation and cooling), business, fire fighting and residential purposes. In many cases, the water supplies for agriculture and industry come from outside the public water supply system, being drawn by the users directly from surface or ground sources. However, in some areas, such users are dependent upon public water supply and for them a failure of the public system could be devastating. Small communities and rural residents often are not served by a public water supply system. Instead, they either have their own wells or are served by private water systems.

Three attributes are crucial to water supply users. There must be water on demand; it must be delivered at sufficient pressure; and it must be safe for use. Actions that affect any of these three factors can be debilitating for the infrastructure.

Contamination of potable water supplies occurs occasionally by accident or from natural causes. Natural blooms of parasites such as Giardia and Cryptosporidium have occurred in many water systems. Such parasites are resistant to treatment with chlorine and therefore require the user to boil water before ingesting it. These blooms are sometimes related to feed lot runoff (the parasites are prolific in the fecal material of farm animals). Naturally occurring blooms generally last for a few days or weeks and then disappear. Some experts voice concern that these parasites, and possibly others, could be introduced deliberately into water systems and cause illness and death in great numbers before the situation could be remedied.

Many common organisms such as *e.coli* are destroyed in the normal water supply environment. An appropriate acidity level (pH) and oxidant level (e.g., chlorine) can destroy many such organisms in less time than they typically remain within the flowing water system. However, there may be bacteria, viruses and other pathogens that can survive this environment to cause sickness and death among the served population. The Commission concluded that there is a credible threat to the nation's water supply systems from certain known biological agents, and that for many potential agents, there is a serious dearth of scientific knowledge needed to assess their threat potential. In addition, there are newly discovered pathogens that emerge under conditions of very high nutrient burden, a condition increasingly common in today's agricultural environment, and their properties are even less well known or understood.

Chemical contamination is also of concern. Several chemical agents have been identified that would constitute credible threats against water supply systems. Although much is known about chemical and biological agents dispersed in air, almost no work has been done on potable waterborne agents. Natural contamination has occurred from surface run off, leaching from toxic waste dumps, or toxic materials, leaking from underground pipes and tanks. These accidental contamination incidents generally have been contained or dealt with successfully.

We have seen no persuasive evidence that purposeful radiological contamination of public water supply systems constitutes an important threat.

The amounts of material needed for purposeful contamination of a water source (such as a large reservoir or aquifer) are considerable and exceed what an individual or small group of terrorists

could easily transport. However, contaminants introduced later would be less susceptible to dilution and would reside in the system for shorter times, thus diminishing the effects of disinfectants and chemical decomposition and oxidation.

Loss of water or water pressure can result from a number of causes. For example, disabling the pumps that maintain flow and pressure, or disabling the electric power sources that run them, could cause long term outages since many of the major pumps and power sources are unique, custom designed equipment that would take months or longer to replace. Fitting more readily available replacement elements might be possible in some situations; however, in several instances we were informed that the engineering difficulties would be serious and that down time would still be on the order of months.

Public potable water systems supply the water for fire fighting in most communities. Loss of water, or even substantial loss of pressure, would disable most fire fighting capability. Some communities have the ability to tap other water sources for fire fighting. For example, fires in Manhattan could be fought by New York's fireboat fleet drawing water from the East River or the Hudson River. Some communities, such as Los Angeles, have large mobile water tankers strategically placed and available to fight fires in case the water system is disabled; the main concern there being earthquakes. Such planning appropriate for natural disasters is largely translatable to other risks. Some communities have mobile pumpers that can withdraw water from storage areas or natural bodies and make it available for fire fighting. Such capabilities, however, are available to only a few cities. Limited capabilities exist to draw water from saltwater sources and transport it to the site of fires. This capability has been used in fighting forest fires in remote locations and probably would be available to urban communities if needed.

Many urban water systems have to rely on a fragile distribution structure. Often referred to as an aging infrastructure, the real problem is that temperature variations, swings in water pressure, vibration from traffic or industrial processes, and accidents often result in broken water mains. Distribution systems in most major cities operate with very little margin. They plan on a number of main breaks based on historical experience. Coordinated attacks on a large number of water mains simultaneously would be difficult to carry out and are not a highly likely threat scenario. However, a system-wide water hammer effect, caused simply by opening or closing major control valves too rapidly, could result in a large number of simultaneous main breaks that exceed the system's capability to respond in a timely manner and would cause widespread outages throughout the community. Recognizing this vulnerability, water systems lately have been incorporating valves that are physically not possible to open or close rapidly. However, many urban systems still have in operation valves that could cause severe water hammer effects.

Finally, interrupting water flow to agricultural and industrial users could have large economic consequences. For example, the California aqueduct, which carries water from northern parts of the state into the Los Angeles/San Diego area, also serves to irrigate the agricultural areas in midstate. Pumping stations are used to maintain the flow of water over rises in terrain. Loss of irrigation water for a growing season, even in years of normal rainfall, would likely result in billions of dollars of loss to California and significant losses to US agricultural exports.

An ancillary problem concerns release of chlorine to the air. Most water supply systems use gaseous chlorine as a disinfectant. The chlorine is normally delivered and stored in railway tank cars. Generally, there is no protection against access to these cars except the overall facility security, which is more often than not minimal. Release of chlorine gas could cause injury to nearby populations.

Foreign ownership of US water supply systems is increasing. But we see no indication of an important vulnerability growing out of this trend.

To summarize, the major vulnerabilities of the nation's water supply systems include susceptibility to contamination and loss of flow and/or pressure resulting from extensive water main breaks, destruction of pumps, or disruption of power supplies.

Emergency Services

This infrastructure includes firefighting, police, rescue, and emergency medical services. Its objectives are to contain and deal with emergencies in order to save lives and preserve property. Except for certain parts of the emergency medical services element, this infrastructure is mostly government owned and operated. It is focused at the local level; state and federal services play an important but supporting role. The infrastructure as defined by the Commission does not include investigative or law enforcement functions, nor does it include activities in the recovery phase**.**

Local police, firefighting and emergency medical services are generally first on the scene of an incident involving public places. Incidents, including accidents, natural disasters, fires or physical attacks involving private facilities, usually are turned over quickly to the emergency services sector because private organizations generally lack the specialized training and resources necessary, and because there may be legal mandates, constraints or consequences of private action. Local authorities faced with large scale incidents turn, where necessary, first to neighboring jurisdictions with whom they have mutual aid agreements for assistance and then, if necessary, to the state. As a general rule, with few exceptions, federal authorities must be invited before they can play a role.

Because of their key role and because time is usually of the essence in dealing with emergencies, the inability of local responders to handle or contain an incident can be a serious vulnerability. It can greatly amplify the effect of the initial event. For example, the inability of a fire department to manage a fire could lead to its spreading and to increased loss of life and property.

The emergency services functions most susceptible to disruption include timely notification of an incident; dispatch of appropriate responders; access to the site; coordination among responders; and effective containment of the incident.

Timely Notification

The 911 system has become popular and is widely used. However, it is susceptible to overload, both by reporting of minor non-emergency incidents and through mischief or malice. There have been several instances where computer viruses that automatically and endlessly dial 911 have been distributed to unsuspecting users. At the programmed time, they flood the system so that it is inoperable. Also, because the system uses the public switched network (PSN) for telecommunications, failures in the PSN can also disable 911.

Fortunately, most major communities do not rely exclusively on the 911 system to provide notification of important incidents. In addition to having alternative telephone numbers, many systems also make use of routine patrols, surveillance (such as through the use of helicopters), reporting by traffic monitors, and even the news media.

Dispatch

In some communities, the dispatch function is centralized. If it is disabled, the ability to notify responders of an incident and to coordinate initial phases of the response is destroyed. Most large cities, however, have redundant and geographically separated dispatch capabilities.

Access to the Site

Traffic congestion in urban areas threatens the ability of emergency systems to respond to incidents. Despite laws and protocols designed to speed emergency responders to their destinations, the flow of traffic often is so heavy that responders suffer significant delays. As cited in the Physical Transportation section of this Appendix, several cities are developing or already using automated traffic control systems, called Intelligent Transportation Systems (ITS), that sense the traffic and control traffic lights to optimize flow and reduce congestion. Such systems can be used to facilitate access to incident sites. However, these advances are two edged: the same automatic system that can control traffic beneficially can be compromised to cause traffic tie-ups and block access by emergency vehicles. These systems appear to have been designed and installed with insufficient regard for security measures needed to prevent or deal with cyber attack.

Coordination

Effective communication among units responding to emergencies is essential for coordinating their efforts. Interoperable communications is needed among police and fire units, medical facilities, and utility or transportation repair crews; across all levels of government; and into the public telephone system. While a wide range of communication options is available, virtually all depend upon having sufficient access to radio frequencies. The bands of frequencies available for public safety are proving to be insufficient due to congestion or interference from other sources.

Today, several bands of radio frequencies are allocated specifically for emergency services, and other bands have been made available for temporary use. The Public Safety Wireless Advisory Committee (PSWAC) concluded in its final report that these existing bands are inadequate. Additional spectrum access is needed to relieve congestion in several urban areas; to facilitate interoperability between existing public safety communications systems; to mitigate interference

problems; and to support migration to modern communications capabilities. In addition, the Federal Communications Commission's (FCC) auctioning of certain frequency bands would force emergency services to move into other spectral ranges, primarily in the 800 MHz band. This would have several undesirable effects. The crowding can produce interference. It would make it easier to jam emergency communications. In cities where there is a high density of large buildings and subsurface systems such as subways, the 800 MHz band—whose signals cannot penetrate concrete and steel structures—is ineffective for emergency communications.

In response to a PSWAC recommendation, the President recently announced an FCC proposal to reallocate the 24 MHz of spectrum currently used by UHF television broadcast channels 63, 64, 68, and 69 for use in public safety communications. Unfortunately, the FCC proposal retains priority of spectrum use for existing and future DTV broadcast stations in these channels; public safety users will have to ensure they cause no interference to television broadcast. Under this proviso, these channels are effectively unavailable to public safety use in several major urban areas. Also, while the FCC's proposal meets the PSWAC recommendation for 24MHz to be made available immediately, it does not address the PSWAC recommendation for up to 66MHz of additional spectrum needed in the future.

Two other factors limit the implementation of interoperable emergency service communications. First, even if additional unencumbered spectrum is made available and a community wants to transition to new frequencies or adopt a new capability, the transition is likely to be costly. Communities faced with such costs may have no alternative but to migrate in stages, which would result in interoperability problems during the entire transition phase. Second, because emergency response in today's world may involve units drawn from a broad regional or even national cross section, interoperability is desirable among all responding units. Approaches will need to be harmonized, geographically across the nation as well as between levels of government. These two factors point to the need for a comprehensive *National Emergency Services Telecommunication Plan* to define common communications approaches, address the financial resources required for the transition, and outline the phasing to minimize interoperability problems during the transition.

Containment and Effectiveness

Based on discussions with local emergency services officials and with national associations, it is apparent that throughout the country there are few, if any, jurisdictions in which first responders feel adequately trained and equipped to meet chemical, biological or radiological incidents. They do not have sensors to tell them they are encountering offending agents or to identify the agent. They do not have adequate protective gear so they cannot be assured of their own safety in dealing with such an incident. They do not have decontamination equipment so they are not able to terminate their own exposure to the agent or that of victims, even after leaving the site. And they do not have sufficient supplies of atropine and other antidotes with which to treat themselves or members of the public who become exposed.

The federal government recognizes this need and provides a number of training and assistance programs for local responders. For example, the Nunn-Lugar-Domincci legislation provides significant funding for a well designed set of program efforts aimed at improving the ability of

local responders to deal with weapons of mass destruction (WMD) incidents. Such efforts need to be intensified and made more widely available more rapidly. Also, there needs to be put in place an affordable mechanism to continually upgrade local capabilities, tracking advances in the capabilities of adversaries.

Containment of fires (and certain other incidents) depends on the availability of water under sufficient pressure. Should the water supply system fail, precious minutes or hours could be lost while alternatives are made available; in most communities, there are no such alternatives.

Often, the federal government has information that can alert local officials to threatening situations and can assist them in preparing for and dealing with incidents. The sharing of information between local and federal levels has not been as effective as it could be. It needs to be improved.

Across the nation, there are federal facilities that have resources that could be important in dealing with emergencies. Traditionally, military base commanders readily provide such resources—food, medical supplies, transportation, manpower, etc.—when needed. However, federal organizations rarely (if ever) participate with nearby organizations in the planning phases of emergency response. This can be important in providing local responders a better understanding of gaps in response capability and procedures for activating federal responses.

Federal capabilities to deal with chemical, biological and radiological incidents are advanced but limited. They can be activated by request originating with the local incident manager, gaining the concurrence of the local mayor and the state governor, and passed along to the Defense Department's Director of Military Support (DOMS) organization. Upon approval, the support mission is assigned to the appropriate base commander, who then orders the unit into action. For planning purposes, it is assumed that a federal team can be on site within 7 to 10 hours after the local incident manager makes his request. There is little practical experience to validate this planning assumption, but given the delays possible in the process, it seems likely that the actual time required to arrive on station could exceed 12 hours. Saving lives in a chemical or biological attack requires a response on the order of minutes. Therefore, no matter how streamlined the activation process, the best solution would appear to be to have such capability at the ready, i.e., pre-positioned based on an expectation or indication of a threat.

In summary, the emergency services infrastructure, which depends heavily upon first responders' capabilities, has fundamental weaknesses that could be exploited to amplify the impact of attacks. These vulnerabilities of the infrastructure can be remedied through more extensive training; access to better technology; better sharing of information; and supplies of critical materiel.

Government Services

Executive Order 13010 designated "continuity of government" as a critical infrastructure. This term has traditionally applied to the survival of our Constitutional form of government in the face of a catastrophic crisis such as nuclear war. In January 1997, a memorandum to the Commission Chairman from the Acting Assistant to the President for National Security Affairs noted that this

traditional concept is distinct from the continuation, in the face of physical and cyber threats to our infrastructures, of services provided by federal, state, and local government. The memorandum stated that it was the latter problem that the Commission was expected to address. Consequently, the Commission has considered *government services* as a critical infrastructure.

Government serves several functions. At the federal level, the Constitution sets forth the responsibilities of government for establishing justice, ensuring domestic tranquillity, providing for the common defense, promoting the general welfare, and securing the blessings of liberty. The constitutions of the 50 sovereign states assign certain parallel responsibilities to the state and local levels. To fulfill these responsibilities, governments at all levels make use of organizations that develop policy, operate programs, regulate, exercise police powers, disburse funds to members of the public, collect taxes, etc. The Commission's focus is on those services of government that are, for the most part, oriented toward promoting the general welfare. This includes, but is not limited to, health and safety as well as disbursements.

Because of time and resource limitations, the Commission has not probed all of the federal, state and local governmental services included in this infrastructure. Emergency services have been dealt with as a separate infrastructure, and to gain an understanding of other government services we sampled Centers for Disease Control (CDC); Social Security Administration(SSA); National Weather Service (NWS); Immigration and Naturalization Service (INS); and state welfare systems.

From the sampled organizations, we draw the following conclusions.

- There is a strong trend toward increased dependency on computer technology, extensive automated databases, ties to the Internet and reliance on the global telecommunications network. Security considerations generally are not high priority.
- Most governmental databases (among government service organizations) contain information relating to individuals and companies and such information is subject to privacy constraints. Vulnerabilities of databases are most likely to be associated with alteration, destruction, or misuse of individual records rather than with global (that is, database wide) effects. At least in the organizations sampled, therefore, it appears very difficult for an outsider to affect more than a small number of records at a time.
- In some cases, physical vulnerabilities may be important.

At the federal government level, the Office of Management and Budget (OMB) has responsibility (under the Paperwork Reduction Act of 1980, as amended) to "develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards and guidelines; evaluate agency information resources management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards and guidelines promulgated by" OMB.

OMB Circular A-130, based on this legislative authority, directs all agencies to, *inter alia*, "protect government information commensurate with the risk and magnitude of harm that could

result from the loss, misuse or unauthorized access to or modification of such information." Agencies are also directed to appoint an individual responsible for strategic information resources management.

While the guidelines provided by OMB are sound, they have not been implemented widely throughout the government. Nor has OMB enforced them.

The National Institute for Standards and Technology (NIST) has the legislated authority to provide assistance in information security to the civilian agencies of the government while the National Security Agency (NSA) has that responsibility for the non-civilian agencies. NSA has pursued its charter enthusiastically and creatively. It has been relatively successful in its program. NIST, residing in a culture that emphasizes academic values and methods, has taken a less aggressive posture and has not obtained resources adequate to its legislated charter in this area. Nevertheless, NIST is developing a set of tests that can be employed to gauge whether information technology products meet certain security and suitability criteria, and has established a program to accredit testing laboratories conducting such tests.

Governments are important purchasers of information technology products. A procurement policy that insists that purchased products undergo rigorous testing and receive appropriate certification would go a long way toward encouraging the private sector to seek such tested and certified products as well.

Major Recommendations

We recommend that the federal role in assuring VHS infrastructures include the following:

- Performing and/or supporting a research and development program to develop needed scientific information on potential contaminants of water supply systems and technology to detect, identify, and treat affected water supply systems. Also, planning and researching on medical treatment of persons exposed to these contaminants through ingestion or absorption through the skin of waterborne agents.
- Providing training and certain equipment, particularly in dealing with chemical, biological and radiological incidents, for local first responders from all jurisdictions likely to face such threats.
- Collecting, analyzing and sharing information concerning threats and vulnerabilities.
- Providing an indications and warning (I&W) system that informs all participants in emergency response of imminent or expected threats and of attacks in progress.
- Raising the level of awareness of the public and of owners and operators of these infrastructures to both physical and cyber attack possibilities and system vulnerabilities, such as ITS vulnerabilities recommended in the Physical Transportation section of this Appendix.
- Making accessible to infrastructures all government owned technology of use in dealing with threats and vulnerabilities of infrastructures.

- Making accessible protective and decontamination gear to first responders.
- Making available stores of atropine and other antidotes.
- Providing information on the identity and location of supporting equipment and replacement equipment, manufacturers of assets at risk, and channels in which to communicate with them.
- Assisting in development of comprehensive Geographical Information Systems (GIS) systems at the local level.
- Encouraging federal government services to assess their vulnerabilities and incorporate adequate attention to security in all plans and operations.
- Ensuring adequate allocation of unencumbered electromagnetic spectrum for public safety telecommunications.
- Designating an entity at federal level (e.g., NTIA) to serve as advocate for the electromagnetic spectrum needs of local and state governments.
- Having FCC and NTIA follow up the PSWAC report recommendation through leading the development of a *National Public Safety Telecommunications Plan* and oversee its implementation.

We recommend state and local governments determine their readiness to deal with incidents, examine vulnerabilities and weaknesses in their systems that could be exploited to amplify the effects of incidents, and apply risk management techniques to deal with potential attacks.

(Intentionally Left Blank)